Dominion KX II-101

用户指南

2.0 版

KX2101-0A-CHS
2008 年 2 月
255-62-4031-00

FCC 信息

本设备已经测试并符合 FCC 规则第 15 部分对有关 A 类数码装置的限制要求。这些限制的设计为商业安装中的有害干扰提供合理保护。本设备产生、使用并辐射无线频率能量，如果不按照说明进行安装和使用，则可能对无线通信产生有害干扰。在居民环境中运行本设备可能产生有害干扰。

VCCI 信息（日本）

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

由于事故、灾害、误用、滥用、对产品进行非 Raritan 的修改或者其他在 Raritan 合理控制范围之外的事件，或并非在正常工作条件下而出现的产品损坏，Raritan 概不承担责任。

C US 1F61
I.T.E.
LISTED

目录

设备管理 105

电源控制 123

安全设置 132

诊断 160

取消 CC 管理 168

规格 171

机架安装 173

索引 179

1 简介

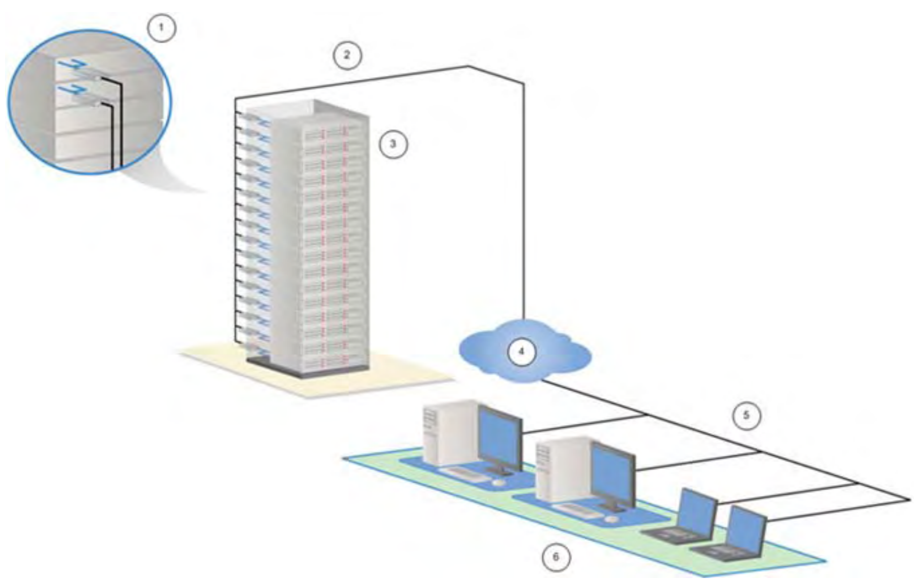
在本章内

Dominion KX II-101 概述

感谢您购买 Dominion KX II-101。KX II-101 提供一个键盘、视频和鼠标 (KVM) 端口连接目标服务器，以及一个 IP 端口连接 IP 网络。在 KX II-101 设备内，来自服务器的 KVM 信号被转换成 IP 格式，经压缩后通过 IP 网络传输。

KX II-101 dongle 结构紧凑，很容易安装在目标服务器附近，每台 KX II-101 设备都有自己的 IP 地址。 每台设备通过 Power-over-Ethernet (PoE) 或外部 AC-DC 电源供电。

Dominion KX II-101 既可以作为独立设备工作，也可以利用 Raritan CommandCenter Secure Gateway (CC-SG) 管理工具，与其他 Raritan 访问产品集成在一个逻辑解决方案里。



1 KX II-101

2 LAN

3 Windows、Linux 和 Sun servers。

4 TCP/IP

5 LAN

6 远程（网络）访问

产品图片







产品特点

接口

- 集成 PS/2 KVM 连接
- 用于控制和虚拟介质的可选 USB 连接
- 用于初始设备设置和诊断与外置调制解调器访问的串行管理端口
- 支持 10/100base-T 自动监测全双工的 Ethernet LAN 端口
- LED 网络活动指示器和状态
- 背光 LED 通电指示器

网络配置

- DHCP 或静态 IP 设备地址

系统管理功能

- 基于 Ethernet 的固件升级
- 故障防护固件升级能力
- 管理员可设置的时钟或网络时间协议 (NTP/SNTP) 同步
- 有时间戳记的本地管理员活动日志 SNMP V2 代理（可由管理员禁用）
- 支持 RADIUS 和 LDAP 验证协议

管理功能

- 基于 Web 的管理
- LDAP、Active Directory、RADIUS 或内部验证和授权
- DHCP 或固定 IP 寻址
- 与 Raritan CommandCenter Secure Gateway (CC-SG) 管理工具集成在一起

用户特点

- 通过常用浏览器进行 Web 访问
- 直观的图形用户界面 (GUI)
- 支持多个远程用户的 PC 共享模式
- TCP 通信
- 英文用户界面
- 虚拟介质访问
- 绝对鼠标同步 (Absolute Mouse Synchronization)
- 即插即用
- 整个 KVM 信号（包括视频和虚拟介质）256 位加密

电源

- 通过二类 Power over Ethernet 供电
- 外部 AC-DC 电源提供替代电源组

视频分辨率

- 60Hz 分辨率下最高为 1600 x 1200

安装

- 机架安装支架

参看***机架安装*** (p. 173)了解详情。

套装内容

每台 KX II-101 设备包括：

- 主机 KX II-101 — 基于 IP Dongle 的 KVM
- USB Type A 到 Type B-mini 连接器
- 电源适配器 — AC-DC 6VDC
- 三个附加电源插头，全球可用
- Mini-DIN 到 DB9 串行电缆
- 安装支架
- Raritan User Manuals & Quick Setup Guides CD-ROM
- 打印版《快速安装指南》
- 打印版《应用说明》（如适用）
- 打印版《技术说明》（如适用）

术语

目标服务器	通过 KX II-101 及其相连的 KVM 配置远程访问的服务器。
远程 PC	用于访问和控制与 KX II-101 相连的目标服务器的 Windows、Linux、Solaris 或 Apple Macintosh® 计算机。
管理串行端口	KX II-101 通过管理串行端口自动配置。用随附的 Mini-DIN 到 DB9 电缆，将 PC 串行端口连接到 KX II-101 设备的管理串行端口。然后用标准仿真软件包（例如 HyperTerminal）访问管理串行端口。 管理串行端口用于进行网络配置。
本地用户端口	使靠近目标服务器的用户无需断开 KX II-101 即可使用本机键盘和鼠标的端口。
虚拟介质	使目标服务器能远程访问客户机 PC 和网络文件服务器上的介质。

任选附件

- DB15 到 PS/2 和 VGA 本地用户电缆

  参看***连接器*** (p. 172)了解详情。

2 重要信息

在本章内

登录

- KX II-101 默认登录用户名是 **admin**，默认密码是 **raritan**。此用户有管理权限。
- 密码区分大小写，必须按创建时使用的大小写组合输入。
- 默认密码 raritan 必须全部以小写字母输入。
- 为了确保安全，要尽快更改默认密码。

默认 IP 地址

KX II-101 的静态默认 IP 地址是 192.168.0.192。在没有 DHCP 服务器的网络上，必须用 KX II-101 串行管理控制台或 KX II-101 Remote Console 配置新的静态 IP 地址、子网掩码和网关地址。

参看***分配 IP 地址*** (p. 21)，了解如何用远程控制台给 KX II-101 分配 IP 地址。参看***使用本地串行控制台*** (参看 "使用终端仿真程序" p. 24)，了解如何用串行管理控制台设置 IP 地址。

服务包

- 使用 Microsoft Internet Explorer v5.01 或 Windows 2000 的 KX II-101 用户必须升级到 Service Pack 4 (SP4) 或更新的服务包。

3 安装和配置

在本章内

配置目标服务器

本章说明如何安装和配置 KX II-101。安装和配置包括下列步骤：

1. ***配置目标服务器*** (p. 7)。
2. ***配置网络防火墙设置*** (p. 19)。
3. ***连接 KX II-101*** (p. 13)。
4. ***配置 KX II-101*** (p. 19)。

为了确保如下所述的最佳性能，要在安装 KX II-101 之前配置要 KX II-101 访问的目标服务器。注意下列配置要求仅适用于目标服务器，不适用于远程访问 KX II-101 的计算机。

设置服务器视频分辨率

为了实现最佳带宽效率和最佳视频性能，应该将运行 Windows、X-Windows、Solaris 和 KDE 等图形用户界面的目标服务器的背景设置为常用的淡色图。应避免使用有照片或复杂渐变图案的背景。

确保 KX II-101 支持服务器的视频分辨率和刷新速率，而且信号为逐行扫描。KX II-101 支持下列视频分辨率：

文本模式	
640x480 @ 60Hz	1024x768 @ 60Hz
640x480 @ 72Hz	1024x768 @ 70Hz
640x480 @ 75Hz	1024x768 @ 75Hz
640x480 @ 85Hz	1024x768 @ 85Hz
800x600 @ 56Hz	1152x864 @ 60Hz
800x600 @ 60Hz	1152x864 @ 75Hz
800x600 @ 72Hz	1280x1024 @ 60Hz
800x600 @ 75Hz	1600x1200 @ 60Hz
800x600 @ 85Hz	

设置 Sun 视频分辨率

Sun Systems 有两种分辨率设置，一种是命令行分辨率，另一种是 GUI 分辨率。如要了解 KX II-101 支持的分辨率，参看***设置服务器视频分辨率*** (p. 8)。

注意：假如支持的分辨率均不起作用，要确保监视器是多同步监视器。某些监视器不使用 H&V 同步。

命令行分辨率

➢ *检查命令行分辨率：*

- 在根目录下运行下列命令：

```
# eeprom output-device
```

➢ *更改命令行分辨率：*

1. 运行下列命令：

```
# eeprom output-device=screen:r1024x768x75
```

其中 1024x768x75 是 KX II-101 支持的任何分辨率。

2. 重新启动计算机。

GUI 分辨率/32 位

➢ *检查 32 位卡的 GUI 分辨率：*

1. 运行下列命令：

```
# /usr/sbin/pgxconfig –prconf
```

➢ *更改 32 位卡的 GUI 分辨率：*

1. 运行下列命令：

```
# /usr/sbin/pgxconfig –res1024x768x75
```

   其中 1024x768x75 是 KX II-101 支持的任何分辨率。

2. 重新启动计算机。

GUI 分辨率/64 位

➢ *检查 64 位卡的 GUI 分辨率：*

1. 运行下列命令：

```
# /usr/sbin/m64config –prconf
```

➢ *更改 64 位卡的分辨率：*

1. 运行下列命令：

```
# /usr/sbin/m64config –res1024x768x75
```

   其中 1024x768x75 是 KX II-101 支持的任何分辨率。

2. 重新启动计算机。

GUI 分辨率/Solaris 8

➢ *检查 32 位卡和 64 位卡的 Solaris 8 分辨率：*

1. 运行下列命令：

```
# /usr/sbin/fbconfig –prconf
```

➢ *更改 32 位卡和 64 位卡的 Solaris 8 分辨率：*

1. 运行下列命令：

```
# /usr/sbin/fbconfig –res1024x768x75
```

   其中 1024x768x75 是 KX II-101 支持的任何分辨率。

2. 重新启动计算机。

鼠标模式

KX II-101 可以在几种鼠标模式下运行：Absolute Mouse Synchronization™（绝对鼠标同步）、智能鼠标模式（不使用动画鼠标）和标准鼠标模式。对于 Absolute Mouse Synchronization，不必修改鼠标参数。对于标准鼠标模式和智能鼠标模式，必须将鼠标参数设置为特定值，本节后面的几段将介绍这些值。

本节介绍不同系统所需的鼠标配置。

Windows Vista

➢ *配置鼠标：*

1. 选择 Start（开始）> Settings（设置）> Control Panel（控制面板）> Mouse（鼠标）。
2. 单击 Pointer Options（指针选项）选项卡。在 Motion（移动）组上：
   a. 将鼠标移动速度精确设置为中速。
   b. 取消选择 Enhanced pointer precision（提高指针精确度）选项。
3. 单击 OK（确定）。

➢ *禁用动画和淡化效果：*

1. 在 Windows Start（开始）菜单上选择 Control Panel（控制面板）> System（系统）> Advanced system settings（高级系统设置）。打开 System Properties（系统属性）对话框。
2. 单击 Advanced（高级）选项卡。
3. 选择 Performance（性能）组里的 Settings（设置）按钮。打开 Performance Options（性能选项）对话框。
4. 在 Custom（定制）选项下，取消选择下列复选框：
   - Animate controls and elements inside windows（窗口用动画显示控件和元素）
   - Animate windows when minimizing and maximizing（在最大化和最小化窗口时用动画显示窗口）
   - Fade or slide menus into view（在视图中淡入淡出或滑动菜单）
   - Fade or slide ToolTips into view（在视图中淡入淡出或滑动工具提示）
   - Fade out menu items after clicking（在单击后淡出菜单项）
5. 单击 OK（确定）。
6. 关闭 Control Panel（控制面板）。

Windows XP 设置

在运行 Microsoft Windows XP 的目标服务器上禁用 Enhanced Pointer Precision（提高指针精确度）选项，将鼠标移动速度准确设置为中速。这些参数可以在 Control Panel（控制面板）> Mouse（鼠标）> Mouse Pointers（鼠标指针）上找到。

注意：对于运行 Windows 2000 或 XP 的目标服务器，您可能要创建一个只用于通过 KX II-101 建立远程连接的用户名。这样，您可以将目标服务器的低速鼠标指针移动/加速设置仅限于 KX II-101 连接。

注意：Windows XP 和 2000 登录屏幕将恢复到与最优 KX II-101 性能对应的建议参数不同的预设鼠标参数，所以在这些屏幕上，鼠标同步不是最佳的。如果您方便调整 Windows 目标服务器上的注册表，可以用 Windows 注册表编辑器更改下列设置：Default user mouse motion speed = 0; mouse threshold 1= 0; mouse threshold 2 = 0，使登录屏幕实现更好的 KX II-101 鼠标同步。

Windows 2000 设置

在运行 Microsoft Windows 2000 的目标服务器上将鼠标指针加速度设置为 none（无），将鼠标移动速度准确设置为中速。这些参数可以在 Control Panel（控制面板）> Mouse（鼠标）上找到。

Linux 设置

在运行 Linux 图形界面的目标服务器上将鼠标加速度准确设置为 1，将阈值准确设置为 1。

如上所述，确保运行 Linux 的每台目标服务器使用 KX II-101 支持的标准 VESA 分辨率和刷新速率。还应该设置 Linux 目标服务器，使消隐时间在 VESA 标准值的+/-40% 范围内。

➢ *检查这些参数：*

1. 转到 Xfree86 配置文件 XF86Config。
2. 用文本编辑器禁用支持的所有非 KX II-101 分辨率。
3. 禁用 KX II-101 不支持的虚拟桌面功能。
4. 检查消隐时间（VESA 标准值的+/-40%）。
5. 重新启动计算机。

注意：在很多 Linux 图形环境下，用 CTRL+ALT++ 命令更改视频分辨率，滚动显示在 XF86Config 文件里启用的所有可用分辨率。

Sun Solaris 设置

必须将目标服务器配置为 KX II-101 支持的其中一个显示分辨率。Sun 计算机支持的最常用的分辨率如下：

1024x768@60Hz

1024x768@70Hz

1024x768@75Hz

1024x768@85Hz

1280x1024@60Hz

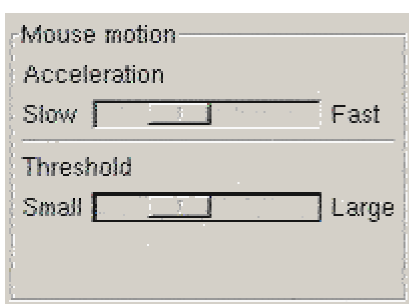
运行 Solaris 操作系统的目标服务器必须输出 VGA 视频（H&V 同步，而非复合同步）。如要将 Sun 显示卡输出从复合同步更改为非默认的 VGA 输出，首先发出 Stop+A 命令进入 bootprom 模式。然后发出下列命令：

#eeprom output-device=screen:r1024x768x75

更改输出分辨率。发出 boot 命令重新引导服务器。

也可以联系 Raritan 代表购买视频输出适配器。使用复合同步输出的 Sun 服务器，需要配备 APSSUN II Raritan Guardian 转换器才能使用 KX II-101。使用不同的复合同步输出的 HD15 Sun 服务器，需要配备 APKMSUN II Raritan Guardian 转换器才能使用 KX II-101。KX101 只支持使用 APSUSB 适配器的 PS/2 版本（不支持复合同步）。

在运行 Solaris 操作系统的目标服务器上将鼠标加速度值准确设置为 1，将阈值准确设置为 1。这既可以在图形用户界面上设置（如下所示），也可以用命令行命令“xset mouse a t”设置，其中“a”是加速度，“t”是阈值。



Apple® Macintosh 设置

使用 Absolute Mouse Synchronization。

连接 KX II-101

KX II-101 的物理连接如下图所示：


1
8
Admin
RESET
2
3
7
Raritan
Dominion
KX2-101
Power
LAN
6
6VDC
PoE
LOCAL USER
4
5

1 随附的监视器和 PS/2 电缆（参看第三项）。

2 Mini-USB 端口。在不使用随附的 PS/2 电缆时，采用随附的 USB 电缆将设备连接到目标服务器。为了使用 Absolute Mouse Sync 或虚拟介质功能，必须使用 USB 连接。

3 随附的监视器和 PS/2 电缆。在不使用 USB 电缆时，用于将设备连接到监视器和目标服务器。

4 LOCAL USER（本地用户）端口。采用可选的 PS/2 电缆，将本地键盘、视频和鼠标直接连接到目标服务器。

5 Ethernet LAN/PoE 端口。在使用 PoE LAN 连接时，提供 LAN 连接和电源。

6 电源连接器。在不使用 PoE (power over Ethernet) LAN 连接时，连接电源。

7 背光 LED 通电和引导指示器。提供设备工作状态反馈。

8 管理端口。用于执行下列操作之一：

用 PC 上的终端仿真程序配置和管理设备。

配置和管理电源板。

连接外置调制解调器，拨号连接该设备。

连接目标服务器

KX II-101 可以用集成 PS/2 电缆或随附的 USB 电缆连接目标服务器。在连接之前，要把目标服务器的视频配置为***设置服务器视频分辨率*** (p. 8) 一节所述的支持的分辨率和刷新速率。

PS/2 配置

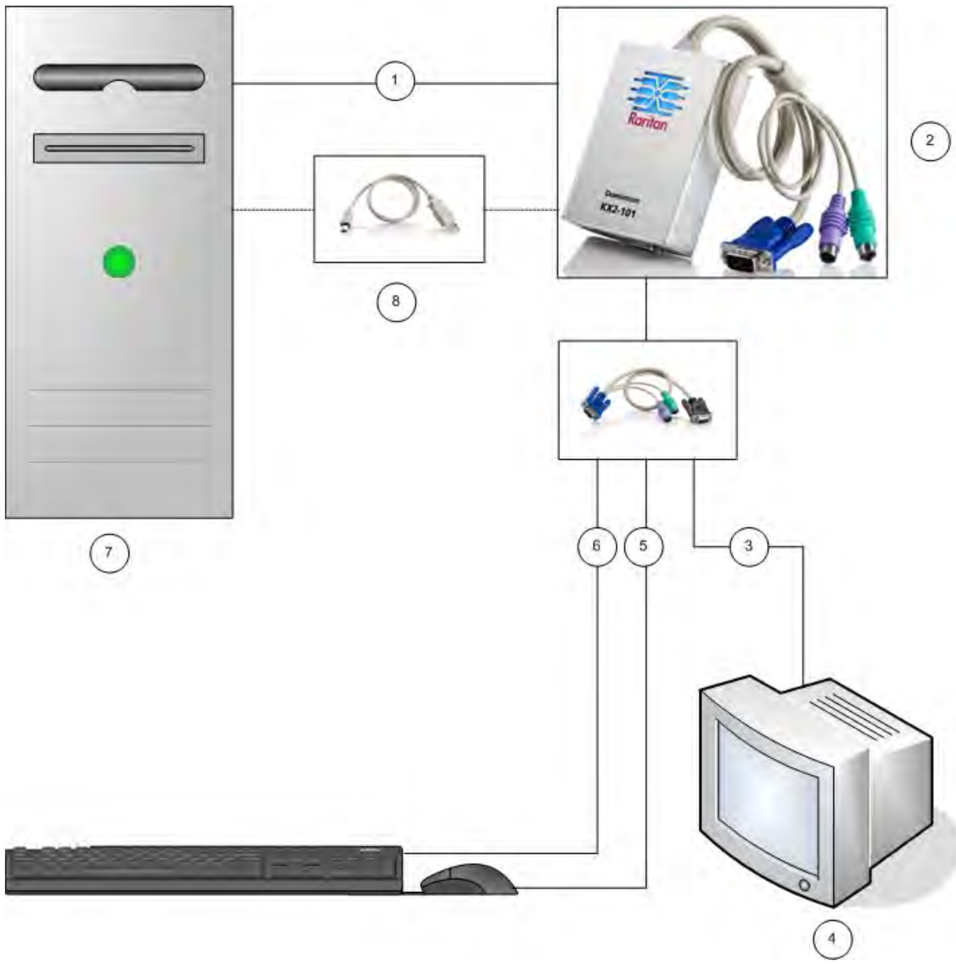
➢ *配置 KX II-101 使用 PS/2 目标服务器:*

1. 用随附的 PS/2 键盘、视频和鼠标电缆将 KX II-101 连接到目标服务器。
2. 用可选的 PS/2 电缆将本地键盘、视频和鼠标连接到 KX II-101 的 Local User（本地用户）端口。

> 注意：KX II-101 必须通电，才能使用 Local User（本地用户）端口。

3. 如果需要虚拟介质连接，将 Mini-USB 连接器连接到 KX II-101，将 USB 连接器连接到目标服务器上的任意 USB 端口。

在连接完成之后，所得到的连接应该如下图所示：



1 从 KX II-101 到目标服务器的集成 PS/2 键盘连接、视频连接和鼠标连接。

2 KX II-101。

3 至本地监视器的视频连接（可选电缆）。

4 本地监视器。

5 从 KX II-101 到鼠标的 PS/2 连接（可选电缆）。

6 从 KX II-101 到键盘的 PS/2 连接（可选电缆）。

7 目标服务器。

8 随附的用于连接 KX II-101 和目标服务器的 Mini-USB 到 USB 连接器，用于实现虚拟介质连接。

USB 配置

➢ *配置 KX II-101 使用 USB 目标服务器：*

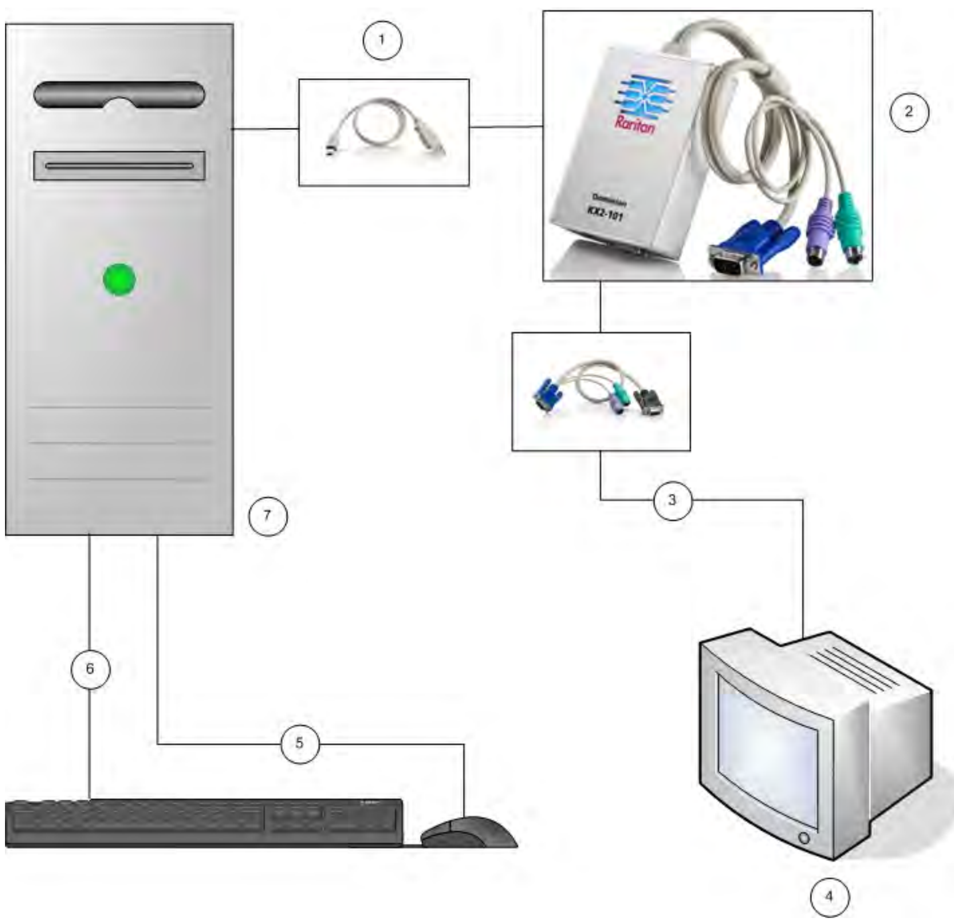
1. 将 Mini-USB 连接器连接到 KX II-101，将 USB 连接器连接到目标服务器上的一个 USB 端口。
2. 用随附的 PS/2 DKX2-101-LPKVMC 电缆仅将本地视频连接到 KX II-101 的 Local User（本地用户）端口。

注意：KX II-101 必须通电，才能使用 Local User（本地用户）端口。

---

3. 用 USB 电缆将键盘和鼠标直接连接到目标服务器。

在连接完成之后，所得到的连接应该如下图所示：



1 随附的用于连接 KX II-101 和目标服务器的 Mini-USB 到 USB 连接器。

2 KX II-101。

3 至本地监视器的视频连接（可选电缆）。

4 本地监视器。

5 从目标服务器到鼠标的 USB 连接。

6 从目标服务器到键盘的 USB 连接。

7 目标服务器。

连接网络

用标准 Ethernet 网线把标记为 LAN 的网络端口连接到 Ethernet 交换机、集线器或路由器上。Ethernet 连接上面的 LAN LED 说明 Ethernet 活动。在使用 KX II-101 时，黄色 LED 闪烁，表示 IP 流量为 10Mbps。绿色指示灯表示 100Mbps 连接速度。

接通 KX II-101 电源

KX II-101 可以用随附的标准交流电源或 PoE (Power over Ethernet) 供电。

- 对于标准交流电源，将随附的交流电源适配器插入 Power Port（电源端口），将另一端插入交流电源插座。
- 对于 PoE，用 10/100Mbps 电缆连接 LAN 端口，将另一端插入支持 PoE 的 LAN。

在 KX II-101 通电之后，要经过引导顺序，蓝色 Raritan 标志 LED 在此过程中将闪烁约 45 秒。 在成功引导之后，背光 LED 保持发光状态不变。

使用管理端口

管理端口允许您使用 HyperTerminal 等终端仿真程序进行 KX II-101 配置和设置。将随附的串行电缆的 Mini-DIN 端插入 KX II-101 的 Admin（管理）端口，将 DB9 端插入 PC 或笔记本的串行端口。串行端口通信设置应该配置为：115,200 波特、8 数据位、1 停止位、无奇偶校验、无流控制。

如要了解如何用 ADMIN（管理）端口配置 KX II-101，参看使用终端仿真程序。

使用本地用户端口

KX II-101 可以使用可选的视频电缆和 PS/2 电缆，通过 LOCAL USER（本地用户）端口将键盘和鼠标连接到目标服务器。LOCAL USER（本地用户）端口充当至（KX II-101 连接的）目标服务器的直通端口，没有其他目的。KX II-101 必须通电，才能使用 Local User（本地用户）。

注意：只有本地端口支持 PS/2 主机接口连接，在用 PS/2 连接器连接到 KX II-101 之后，必须重新启动目标服务器。

配置网络防火墙设置

如要通过网络防火墙访问 KX II-101，防火墙必须允许在 TCP 端口 5000 上进行通信。还可以配置 KX II-101 使用另一个你自己分配的 TCP 端口。

为了充分利用 KX II-101 的 Web 访问功能，防火墙必须允许 TCP 端口 443 接受入站通信，该端口是用于 HTTPS 通信的标准 TCP 端口。为了充分利用 KX II-101 的 HTTP 到 HTTPS 重定向（用户可以输入更常用的 http://xxx.xxx.xxx.xxx，而不是 https://xxx.xxx.xxx.xxx），防火墙还必须允许 TCP 端口 80 接受入站通信，该端口是用于 HTTP 通信的标准 TCP 端口。

配置 KX II-101

KX II-101 可以采用两种方式配置：

- 使用 KX II-101 Remote Console，它要求设备有网络连接与工作站相连。
- 使用 HyperTerminal 等终端仿真程序，它要求设备的 ADMIN（管理）端口直接连接工作站。本连接所用的电缆随 KX II-101 一起提供。

本节介绍 KX II-101 的两种配置方法。

使用远程控制台

KX II-101 Remote Console 是基于 Web 的应用程序，您可以在配置设备之后，在使用和管理设备之前用它配置设备。在用远程控制台配置 KX II-101 之前，必须将工作站和设备与网络相连。

为了配置 KX II-101，您：

- 设置新密码取代默认密码
- 分配 IP 地址
- 命名目标服务器
- 创建用户和组

设置新密码

在首次登录远程控制台时，提示您设置新密码取代默认密码。然后即可配置 KX II-101。

1. 登录到与 KX II-101 设备相连的工作站。
2. 启动支持的网络浏览器，例如 Internet Explorer (IE) 或 Firefox。
3. 在浏览器地址栏输入设备的默认 IP 地址：

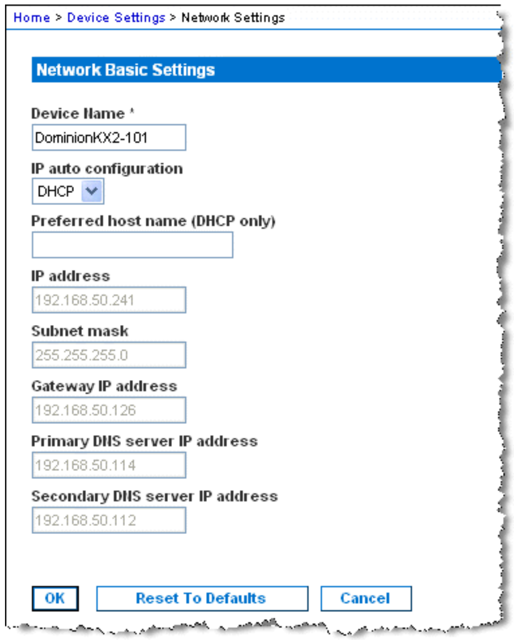
   192.168.0.192
4. 按 Enter 键。打开登录页面。
5. 输入用户名 `admin` 和密码 `raritan`。
6. 单击 Login（登录）。

   显示 Change Password（更改密码）页。
7. 在 Old Password（旧密码）字段里输入 raritan。
8. 在 New Password（新密码）字段里输入新密码，在 Confirm New Password（确认新密码）字段里重新输入新密码。密码最长为 64 个字符，可以包含英文字母数字和可打印的特殊字符。
9. 单击 Apply（应用）。

   将显示确认信息，说明密码更改成功。
10. 单击 OK（确定）。打开 Port Access（端口访问）页。

分配 IP 地址

1. 在 KX II-101 Remote Console 上选择 Device Settings（设备设置）> Network Settings（网络设置）>。打开 Network Basic Settings（网络基本设置）页。



2. 在 Device Name（设备名称）字段里给 KX II-101 设备指定一个有意义的名称，设备名称最多为 16 个字母数字和特殊字符，不能包含空格。

3. 在 IP auto configuration（IP 自动配置）下拉列表上选择 IP 配置：

   - None (Static IP)（无 [静态 IP]）。这是默认值和建议的选项，因为 Dominion KX II-101 是基础架构设备，其 IP 地址不应变化。此选项要求您人工指定网络参数。
   - DHCP。如果使用此选项，每当引导 KX II-101 时，网络参数由 DHCP 服务器分配。

配置直接端口访问

➢ *配置直接端口访问：*

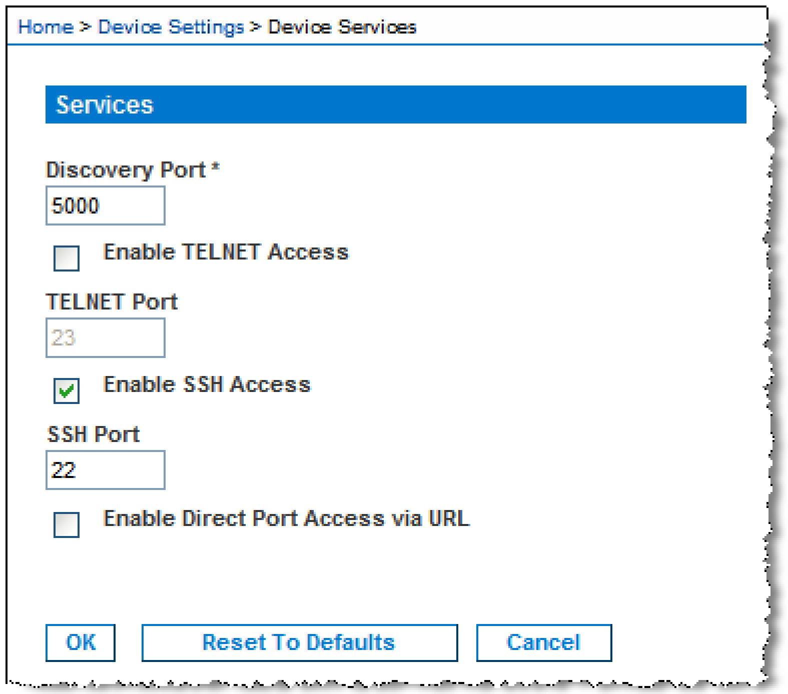
1. 选择 Device Settings（设备设置）> Device Services（设备服务）。打开 Device Services（设备服务）页。

2. 选择 Enable Direct Port Access via URL（通过 URL 启用端口访问）复选框。

3. 启用全局 Telnet 或 SSH 访问。

- 选择 Enable TELNET Access（启用 TELNET 访问）复选框启用 TELNET 访问。
- 选择 Enable SSH Access（启用 SSH 访问）复选框启用 SSH 访问。

4. 给选择的访问类型指定一个有效 TCP 端口。例如通过 Telnet TCP 端口的直接端口访问可以配置为 7770。

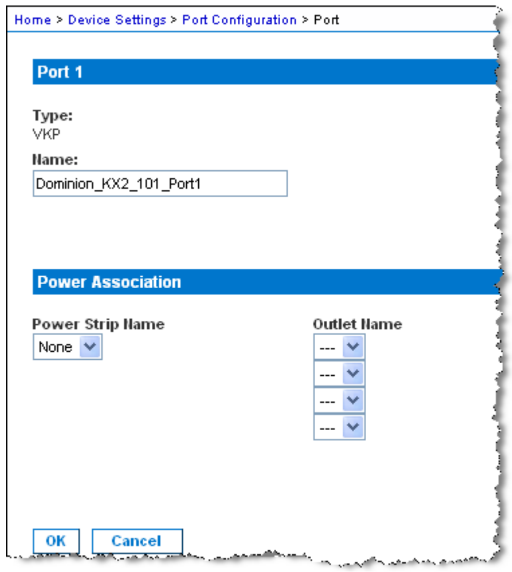


5. 单击 OK（确定）按钮保存此信息。

命名目标服务器

1. 如***连接 KX II-101*** (p. 29) 一节所述，将 KX II-101 连接到目标服务器（如还没有连接）。
2. 选择 Device Settings（设备设置）> Port Configuration（端口配置）。打开 Port Configuration（端口配置）页。

3. 单击目标服务器的 Port Name（端口名称）。打开 Port（端口）页。



4. 输入名称（最多 32 个字母数字和特殊字符）。
5. 单击 OK（确定）。

创建用户和组

用户组可用来进行本地和远程验证（通过 RADIUS 或 LDAP）。在创建个人用户之前，最好先定义用户组，因为在添加用户时，必须给该用户指定一个现有用户组。

➢ *创建用户组：*

1. 用下列方法之一打开 Group（组）页：
   a. 选择 User Management（用户管理）> Add New User Group（添加新用户组），或者
   b. 单击 User Group List（用户组列表）页上的 Add（添加）按钮。
2. 在 Groupname（组名）字段里输入新用户组的描述性名称。
3. 给该组设置 Permissions（权限）。选择要分配给该组中所有用户的权限前面的复选框。
4. 设置 Port Permissions（端口权限）（Access [访问]、VM Access [VM 访问]和 Power Control [电源控制]）。指定本组用户可以访问的服务器端口和访问类型。请注意 VM（虚拟介质）访问的默认值像所有端口权限一样，是 off（关）。如要使用虚拟介质，必须启用适当的权限。
5. 单击 OK（确定）。

➢ *创建新用户：*

1. 用下列方法之一打开 User（用户）页：
   a. 选择 User Management（用户管理）> Add New User（添加新用户），或者
   b. 单击 User List（用户列表）页上的 Add（添加）按钮。
2. 在 Username（用户名）字段里输入一个唯一名称（最长 16 个字符）。
3. 在 Full Name（全名）字段里输入该用户的全名（最长 64 个字符）。
4. 在 Password（密码）字段里输入密码，在 Confirm Password（确认密码）字段里重新输入密码（最长 64 个字符）。
5. 在 User Group（用户组）下拉列表上选择组。除了系统提供的默认组（Admin [管理员]、<Unknown [未知]>和 Individual Group [个人组]），此列表还包含您创建的所有组。如果您不想使此用户与现有 User Group（用户组）关联，在 Individual Group（个人组）下拉列表上选择个人组。
6. 单击 OK（确定）。

使用终端仿真程序

可以用管理串行控制台和 HyperTerminal 等终端仿真程序设置 KX II-101 的下列配置参数。

- IP 地址
- 子网掩码地址
- 网关地址
- IP 访问控制
- LAN 速度
- LAN 接口模式

为了与 KX II-101 一起使用终端仿真程序，必须首先用随附的 RS-232 串行电缆把 KX II-101 的 Admin（管理）端口连接到 PC 的 COM1 端口。参看***使用管理端口*** (p. 18)了解详情。

为了说明问题，本节以 HyperTerminal 为例说明终端仿真程序。您可以使用任何终端仿真程序。

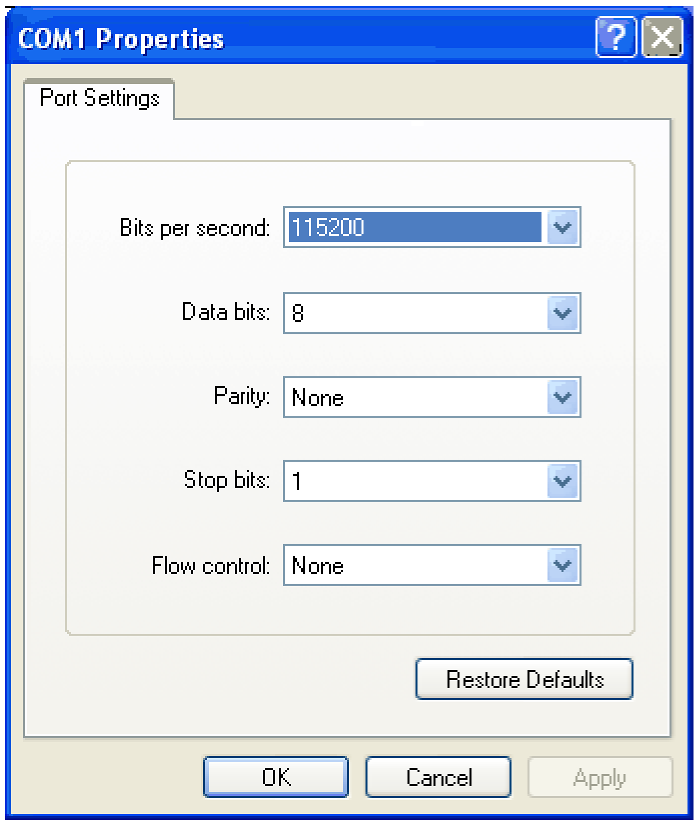
➢ *用终端仿真程序配置 KX II-101：*

1. 用随附的 RS-232 串行电缆将 KX II-101 连接到本地 PC。

   将 KX II-101 的 Admin（管理）端口连接到 PC 的 COM1 端口。
2. 启动要用于配置 KX II-101 的终端仿真程序：

3. 用终端仿真程序设置下列端口设置：

- Bits per second（比特率）：115200
- Data bits（数据位）：8
- Parity（奇偶校验）：None（无）
- Stop bits（停止位）：1
- Flow control（流控制）：None（无）



4. 连接 KX II-101。

显示登录屏幕。



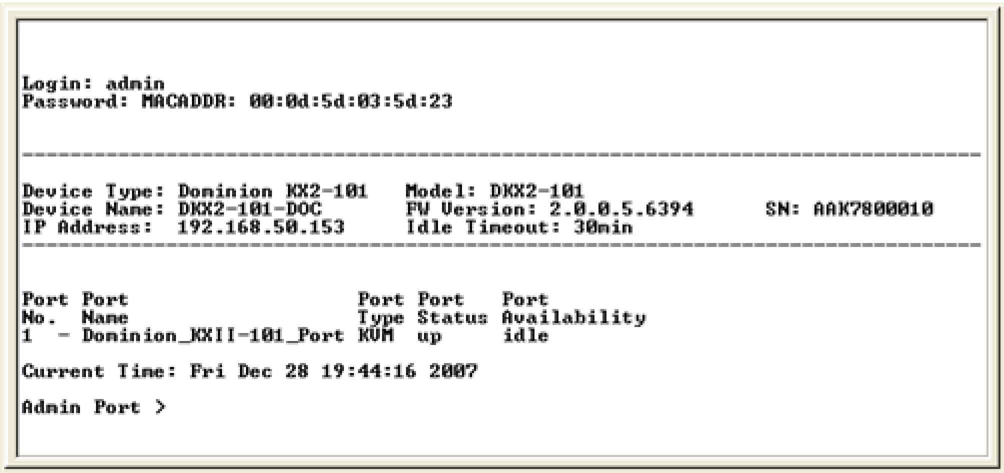
5. 输入管理员用户名，按 Enter 键。

系统提示您输入密码。



6. 输入密码，按 Enter 键。

显示 Admin Port（管理端口）提示符。



```
Login: admin
Password: MACADDR: 00:0d:5d:03:5d:23

--------------------------------------------------------------------------------

Device Type: Dominion KX2-101    Model: DKX2-101
Device Name: DKX2-101-DOC        FW Version: 2.0.0.5.6394      SN: AAK7800010
IP Address:  192.168.50.153      Idle Timeout: 30min
--------------------------------------------------------------------------------

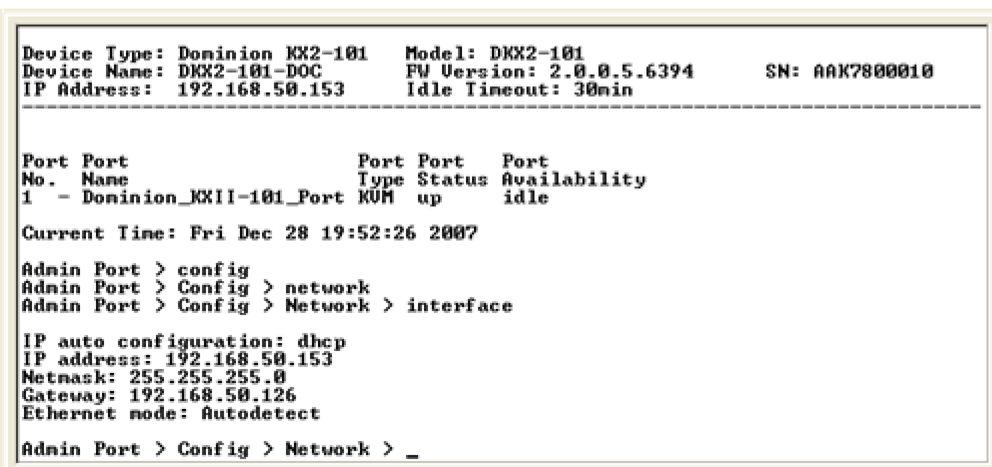
Port Port                        Port Port   Port
No.  Name                        Type Status Availability
1  - Dominion_KXII-101_Port      KVM  up     idle

Current Time: Fri Dec 28 19:44:16 2007

Admin Port >
```

7. 在 Admin Port（管理端口）> 提示下输入 `config`，按 Enter 键。
8. 在 Config > 提示下输入 `network`，按 Enter 键。
9. 如要查看当前接口设置，在 Interface（接口）> 提示下输入 `interface`，按 Enter 键。

   显示当前接口设置：



```
Device Type: Dominion KX2-101    Model: DKX2-101
Device Name: DKX2-101-DOC        FW Version: 2.0.0.5.6394      SN: AAK7800010
IP Address:  192.168.50.153      Idle Timeout: 30min
--------------------------------------------------------------------------------

Port Port                        Port Port   Port
No.  Name                        Type Status Availability
1  - Dominion_KXII-101_Port      KVM  up     idle

Current Time: Fri Dec 28 19:52:26 2007

Admin Port > config
Admin Port > Config > network
Admin Port > Config > Network > interface

IP auto configuration: dhcp
IP address: 192.168.50.153
Netmask: 255.255.255.0
Gateway: 192.168.50.126
Ethernet mode: Autodetect

Admin Port > Config > Network > _
```

10. 如要配置新网络设置，在 Network（网络）提示下输入 `interface`，后跟下列其中一个命令及其适当的自变量（选项），按 Enter 键。

命令	自变量	选项
ipauto	none|dhcp	none — 允许您人工指定设备的 IP 地址。必须在此选项之后使用 ip 命令和 IP 地址，如下列例子所示： `interface ipauto none ip 192.168.50.12` dhcp — 在启动时自动给设备分配 IP 地址。

命令	自变量	选项
ip	IP address	给设备分配的 IP 地址。在首次人工设置 IP 地址时，必须使用此命令与 ipauto 命令和 none 选项。参看 ipauto 了解详情。在人工分配 IP 地址之后，可以单独用 ip 命令更改 IP 地址。
mask	subnetmask	子网掩码 IP 地址。
gw	IP address	网关 IP 地址。
mode	mode	Ethernet 模式。可以使用下列选项： auto — 自动根据网络设置速度和接口模式。 10hdx — 10Mbps 半双工。 10fdx — 10Mbps 全双工。 100hdx — 100Mbps 半双工。 100fdx — 100Mbps 全双工。

在成功更改设置之后，显示下面这样的确认消息：

```
Admin Port > config
Admin Port > Config > network
Admin Port > Config > Network > interface ipauto none ip 192.168.50.126
Network interface configuration successful.
```

1. 在完成 KX II-101 配置之后，在命令提示下输入 logout，按 Enter 键。

   您退出命令行界面。

4 连接 KX II-101

在本章内

语言支持

KX II-101 提供下列语言键盘支持：美国英语、繁体中文、简体中文、日语、朝鲜语、法语和德语。

注意：中文、日语和朝鲜语键盘只用于显示；KX II-101 Remote Console 功能目前不支持本地语言输入。

Linux 语言配置

参看 **KVM 和串行访问客户机用户指南**中的*键盘类型*，了解如何在 Linux 服务器上配置外文键盘。

Java Runtime Environment (JRE)

重要事项：建议您禁用 Java 高速缓存，清除 Java 高速缓存。请参看 Java 文档或《Raritan Multi-Platform Client (MPC) 和 Raritan Remote Client (RRC) 用户指南》了解详情。

KX II-101 Remote Console 和 MPC 需要 JRE 才能运行。KX II-101 Remote Console 检查 Java 版本；如果版本错误或陈旧，会提示您下载兼容版本。

Raritan 建议您使用 Java Runtime Environment (JRE) v1.5 实现最佳性能，但 KX II-101 Remote Console 和 MPC 将使用 JRE v1.4.2_05 或更高版本（JRE 1.5.0_02 除外），包括 JRE 1.6.x，但不包括 1.6.2。

注意：为了在 KX II-101 Remote Console (Virtual KVM Client) 上使用多语言键盘，请安装多语言版本的 Java Runtime Environment (JRE)。

启动 KX II-101

重要事项：无论使用什么浏览器，都必须允许 Dominion 设备 IP 地址弹出窗口，这样才能启动 KX II-101 Remote Console。

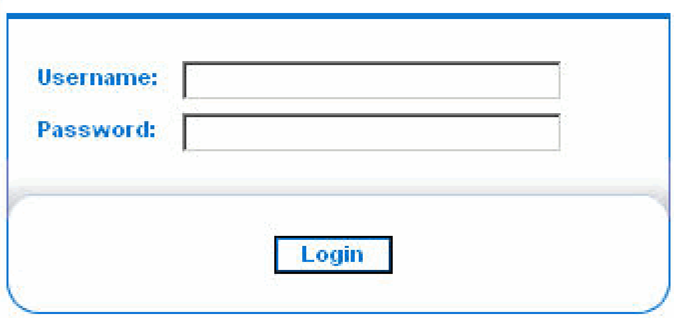
您可能会看到各种安全警告和证书警告，视浏览器和安全设置而定。必须接受这些警告，才能启动 KX II-101 Remote Console。

您可以在这些安全和证书警告消息上选择下列选项，减少在随后的登录中弹出的警告消息数：

- In the future, do not show this warning（不再显示此警告）
- Always trust content from this publisher（总是信任来自此发行商的内容）

➢ *启动 KX II-101 Remote Console：*

1. 登录到与 KX II-101 设备相连并安装了 Java Runtime Environment v1.4.2_05 或更高版本（JRE 可在 ***http://java.sun.com/*** http://java.sun.com 下载）的任何工作站。
2. 启动支持的网络浏览器，例如 Internet Explorer (IE) 或 Firefox。
3. 输入下列 URL：http://IP-ADDRESS，其中 IP-ADDRESS 是您给 KX II-101 设备分配的 IP 地址。也可以使用 https，管理员分配的 KX II-101 DNS 名称（假定配置了 DNS 服务器），或者只在浏览器地址栏输入 IP 地址（KX II-101 始终将 IP 地址由 HTTP 重定向到 HTTPS）。打开 Logon（登录）页。



4. 输入用户名和密码。如果是首次登录，用出厂默认用户名和密码（admin 和 raritan [全部为小写字母]）登录；系统将提示您更改默认密码。参看更改默认密码了解详情。
5. 单击 Login（登录）。

启用直接端口访问

直接端口访问允许您直接访问 KX II-101 Remote Client，无需使用常用的登录页。在启用直接端口访问之后，您可以定义一个 URL，直接导航到 Port Access（端口访问）页。

➢ *启用直接端口访问：*

1. 启动 KX II-101 Remote Console。
2. 选择 Device Settings（设备设置）> Device Services（设备服务）。打开 Device Services（设备服务）页。
3. 选择 Enable Direct Port Access via URL（通过 URL 启用直接端口访问）复选框。
4. 单击 Save（保存）按钮保存设置。

➢ *定义直接端口访问 URL：*

- 用 KX II-101 的 IP 地址、用户名、密码和端口号（必要时）定义一个 URL。

  如果只有一个 KVM 端口，不需要端口号。

  直接端口访问 URL 的格式如下：

  https://[**IP address**]/dpa.asp?username=[**username**]&password=[**password**]&port=[**port number**]

提示：一旦定义直接端口访问 URL，就在浏览器里把它保存成书签，便于重复使用。

KX II-101 控制台布局

KX II-101 Remote Console 提供一个供配置和管理使用的 HTML（类似 Web）界面，还提供目标服务器列表和选择。所有选项分布在各个选项卡上。

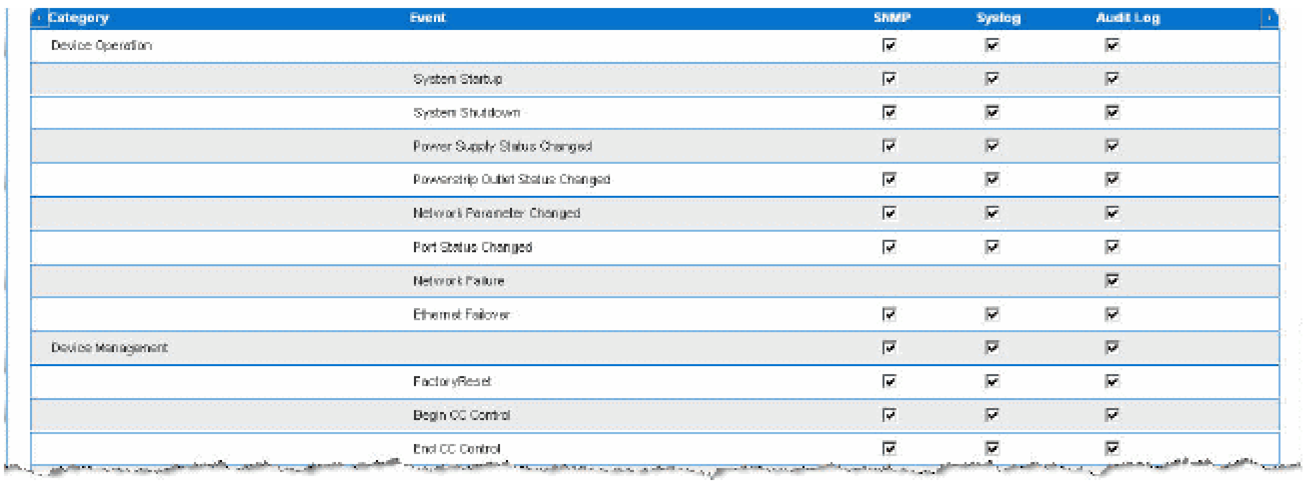
成功登录之后，打开 Port Access（端口访问）页，显示端口及其状态和可用性。

KX II-101 控制台导航

KX II-101 Remote Console 界面提供多种导航和选择方法。

➢ *选择一个选项（使用下列任何一种方法）：*

- 单击一个选项卡，打开一页可用选项。
- 把鼠标放在选项卡上，在菜单上选择适当的选项。
- 直接单击分层显示菜单（导航路径）上的选项。

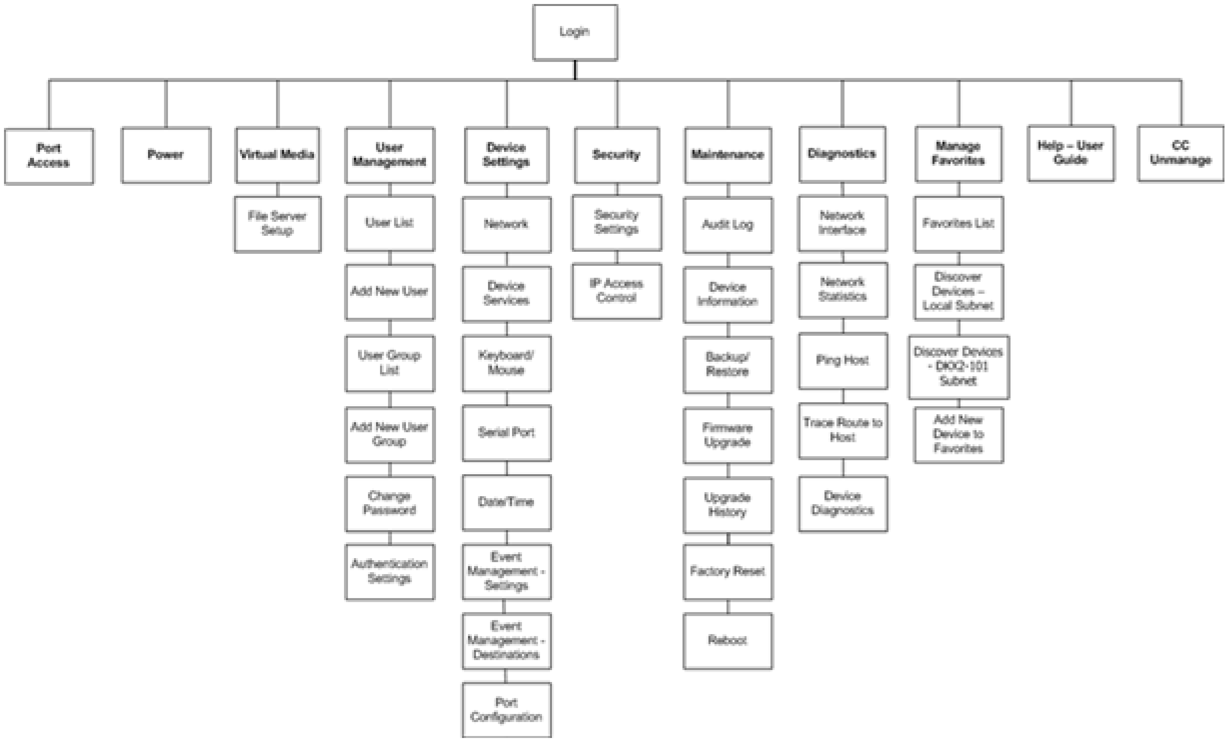


➢ *滚动超过一屏的页面：*

- 使用键盘上的 Page Up 键和 Page Down 键，或者
- 使用右边的滚动条

KX II-101 Remote Console 菜单图

下图说明 KX II-101 Remote Console 上的所有可用菜单选项。



注销

➢ *退出 KX II-101 Remote Console：*

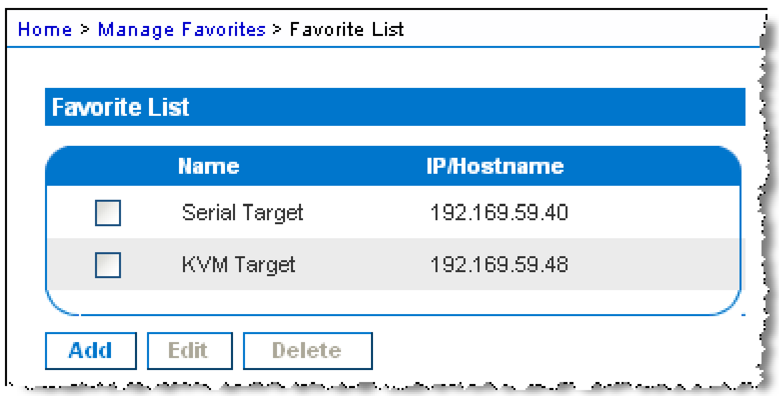
- 单击页面右上角的 Logout（注销）。

注意：注销时，关闭打开的所有 Virtual KVM Client 会话和串行客户机会话。

管理收藏夹

提供收藏夹功能的目的是让您组织和快速访问常用的设备。Favorite Devices（收藏设备）部分位于 Port Access（端口访问）页左下部（侧面工具栏），具备下列功能：

- 创建和管理收藏设备列表
- 快速访问常用设备
- 按名称或 IP 地址列出收藏设备
- 在子网上发现 KX II-101 设备（登录前后）
- 在连接设备中检索发现的 KX II-101 设备（登录后）



➢ *访问收藏的 KX II-101 设备：*

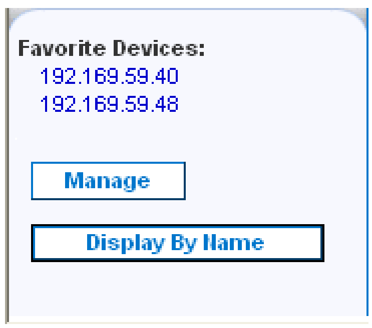
- 单击该设备的设备名称（列在 Favorite Devices [收藏设备]下）。针对该设备打开新浏览器窗口。

➢ *在名称和 IP 地址之间切换 Favorite Devices（收藏设备）列表显示：*

按 IP 地址显示收藏夹：

单击 Display by IP（按 IP 地址显示）按钮。

Favorite Devices（收藏设备）当前按名称显示，单击 Display by IP（按 IP 地址显示）按钮切换显示方式。



按名称显示收藏夹：

单击 Display by Name（按名称显示）按钮。

Favorite Devices（收藏设备）当前按 IP 地址显示，单击 Display by Name（按名称显示）按钮切换显示方式。



管理收藏夹菜单

➢ *打开 Manage Favorites（管理收藏夹）菜单：*

- 单击 Manage（管理）按钮。打开 Manage Favorites（管理收藏夹）页，该页包括：

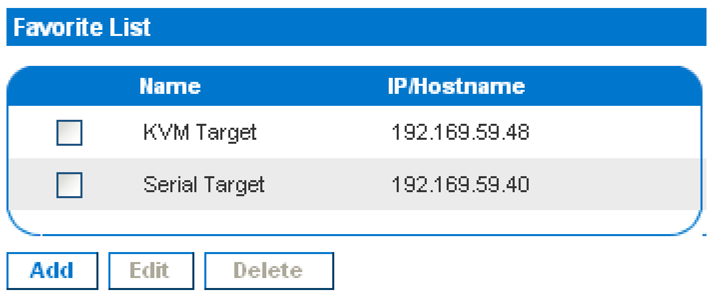
使用：	目的：
Favorites List（收藏夹列表）	管理收藏设备列表。
Discover Devices - Local Subnet（发现设备 - 本地子网）	发现本地子网上的设备。
Discover Devices - KX II-101 Subnet（发现设备 — KX II-101 子网）	发现 KX II-101 设备子网上的设备。
Add New Device to Favorites（将新设备添加到收藏夹）	在收藏夹列表上添加、编辑和删除设备。

收藏夹列表

在 Favorites List（收藏夹列表）页上，可以在收藏夹列表上添加、编辑和删除设备。

➢ *打开 Favorites List（收藏夹列表）页：*

- 选择 Manage（管理）> Favorites List（收藏夹列表）。打开 Favorites List（收藏夹列表）页：



➢ *添加收藏夹：*

- 单击 Add（添加）按钮。打开***添加新收藏夹*** (p. 41)页。

➢ *删除收藏夹：*

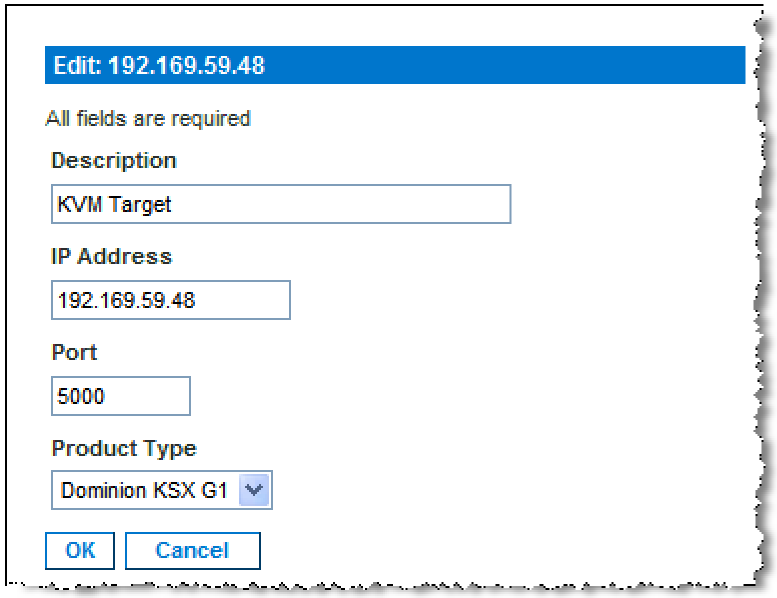
重要事项：在删除收藏夹时要小心谨慎，系统不提示您确认删除。

1. 选择适当的 KX II-101 设备旁边的复选框。
2. 单击 Delete（删除）按钮。收藏夹从收藏夹列表上删除掉。

➢ *编辑收藏夹：*

1. 在 Favorites List（收藏夹列表）页上，选择适当 KX II-101 设备旁边的复选框。

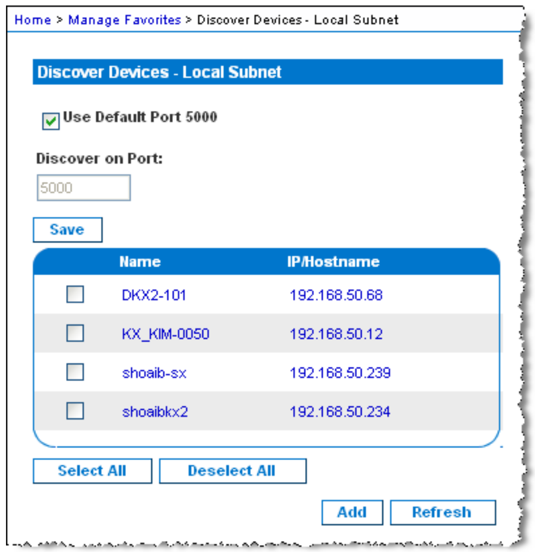
2. 单击 Edit（编辑）按钮。打开 Edit（编辑）页：



3. 按需要更新字段：
   - Description（说明）。输入有意义的内容。
   - IP Address（IP 地址）。输入 KX II-101 设备的 IP 地址。
   - Port（端口）。更改发现 Port（端口）（如有必要）。
   - Product Type（产品类型）。
4. 单击 OK（确定）。

发现设备 — 本地子网

此选项用于发现本地子网（即运行 KX II-101 Remote Console 的子网）上的设备；可以直接在本页上访问这些设备，或者将它们添加到收藏夹列表里。



➢ *发现本地子网上的设备：*

1. 选择 Favorites（收藏夹）> Discover Devices - Local Subnet（发现设备 — 本地子网）。打开 Discover Devices - Local Subnet（发现设备 — 本地子网）页。
2. 选择适当的发现端口（参看网络其他设置了解发现端口）：
   - 如要使用默认发现端口，选择 Use Default Port 5000（使用默认端口 5000）选项。
   - 使用不同的发现端口：

   a. 取消选择 Use Default Port 5000（使用默认端口 5000）选项。

   b. 在 Discover on Port（发现端口）字段里输入端口号。

   c. 单击 Save（保存）。
3. 单击 Refresh（刷新）。刷新本地子网上的设备的列表。

➢ *将设备添加到收藏夹列表：*

1. 选择设备名称/IP 地址旁边的复选框。
2. 单击 Add（添加）。

提示：用 Select All（全选）和 Deselect All（取消全选）按钮快速选择（或取消选择）远程控制台子网上的所有设备。

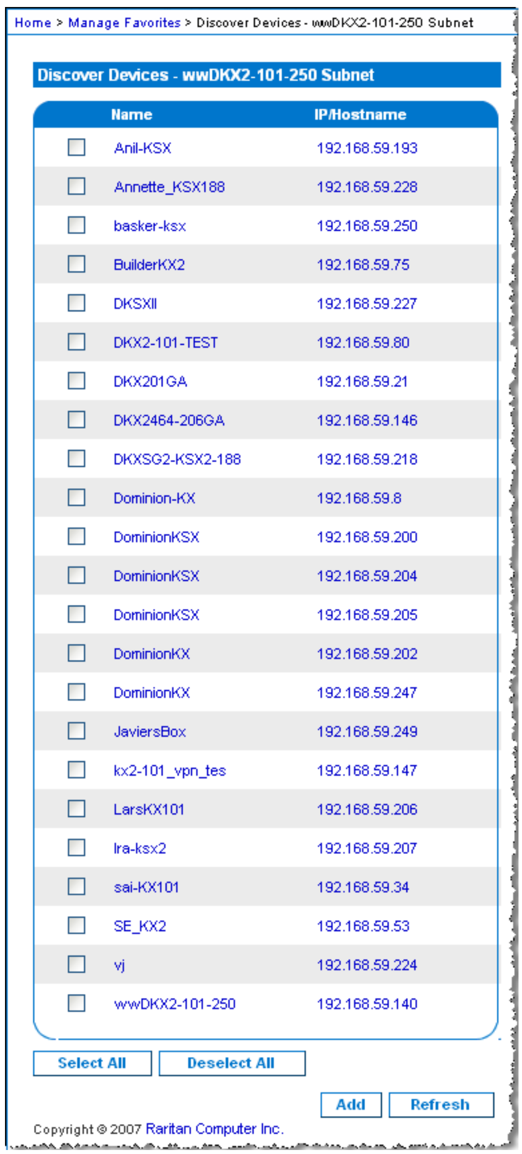
➢ *访问发现的设备：*

- 单击该设备的设备名称或 IP 地址。针对该设备打开新浏览器窗口。

发现设备 — KX II-101 子网

此选项用于发现设备子网（即 KX II-101 设备 IP 地址自身的子网）上的设备；可以直接在该页上访问这些设备，或者将它们添加到收藏夹列表里。

此功能使多台 KX II-101 设备能互操作并自动伸缩。KX II-101 Remote Console 自动发现 KX II-101 子网上的 KX II-101 设备。



➢ *发现设备子网上的设备：*

1. 选择 Favorites（收藏夹）> Discover Devices - Local Subnet（发现设备 — KX II-101 子网）。打开 Discover Devices — KX II-101 Subnet（发现设备 — KX II-101 子网）页。
2. 单击 Refresh（刷新）。刷新本地子网上的设备的列表。

➢ *将设备添加到收藏夹列表：*

1. 选择设备名称/IP 地址旁边的复选框。
2. 单击 Add（添加）。

提示：用 Select All（全选）和 Deselect All（取消全选）按钮快速选择（或取消选择）KX II-101 设备子网上的所有设备。

➢ *访问发现的设备：*

- 单击该设备的设备名称或 IP 地址。针对该设备打开新浏览器窗口。

添加新收藏夹

➢ *将设备添加到收藏夹列表：*

1. 选择 Manage Favorites（管理收藏夹）> Add New Device to Favorites（将新设备添加到收藏夹）。打开 Add New Favorite（添加新收藏夹）页：
2. 输入有意义的 Description（说明）。
3. 输入该设备的 IP Address（IP 地址）。
4. 更改发现 Port（端口）（如有必要）。
5. 单击 OK（确定）。

   此设备被添加到收藏夹列表里。

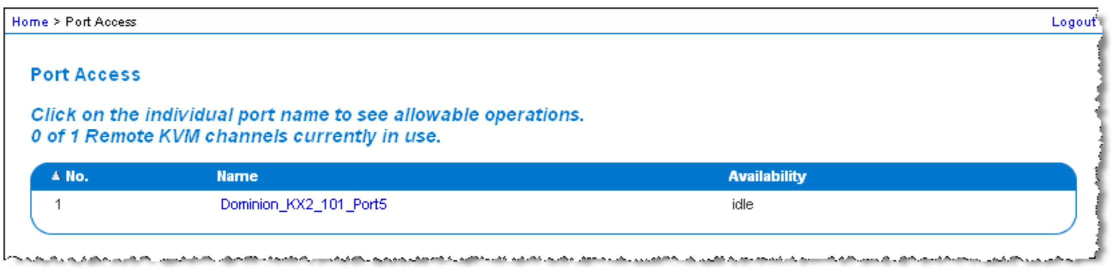
端口访问页

在成功登录 KX II-101 Remote Console 之后，打开 Port Access（端口访问）页。本页显示 KX II-101 端口及其状态和可用性。Port Access（端口访问）页提供对与 KX II-101 相连的目标服务器的访问。KVM 目标服务器是您要通过 KX II-101 设备控制的服务器，它用随附的设备上的 PS/2 连接器连接到 KX II-101。

注意：对于目标服务器的每个连接，打开一个新的 Virtual KVM Clien 窗口。

➢ *使用端口访问页：*

1. 在 KX II-101 Remote Console 上单击 **Port Access（端口访问）**选项卡。打开 **Port Access（端口访问）**页：



- No.（序号）。只有一个端口可供 KX II-101 使用。
- Name（名称）。KX II-101 端口的名称；最初设置为 Dominion_KX101G2_Port1，但可以将此名称更改为更具说明性的名称。
- Availability（可用性）。可用性可以是 Idle（空闲）、Connected（已连接）、Busy（忙）或 Unavailable（不可用）。

2. 如要连接目标服务器，单击设备/目标服务器的名称，然后单击 Connect（连接）弹出窗口。打开 Virtual KVM Client 窗口，可用性变成 Busy（忙）。
3. 如要断开目标服务器，单击设备/目标服务器的名称，然后单击 Disconnect（断开）弹出窗口。关闭 Virtual KVM Client 窗口，可用性变成 Idle（空闲）。

5 用户、组和访问权

在本章内

用户

KX II-101 在内部存储所有用户名和组名的列表，以便确定访问授权和权限。这些信息以加密形式存储在内部。有几种验证方式，其中一种是本地验证。所有用户必须接受验证；如果 KX II-101 配置为用 LDAP 或 RADIUS 进行验证，将首先处理这些验证，然后处理本地验证。

如要访问 KX II-101 设备，必须输入用户名和密码。这些信息用于验证那些尝试访问 KX II-101 设备的用户。参看***用户管理*** (p. 44)，了解如何添加和编辑用户。

组

每台 KX II-101 设备有三个默认用户组，不能删除这些用户组：

User（用户）	Description（说明）
Admin（管理员）	该组里有全部管理权限的用户。原始出厂默认用户是该组的成员，具有全部系统权限。此外，管理员用户必须是管理员组的成员。
Unknown（未知）	这是在外部用 LDAP/LDAPS 或 RADIUS 验证的或系统不知道的默认用户组。如果外部 LDAP/LDAPS 或 RADIUS 服务器无法确定有效用户组，就使用 Unknown（未知）组。此外，新创建的所有用户均属于此组，直到给他们指定另一个组为止。
Individual Group（个人组）	个人组实际上是只有一个用户的组。也就是说，某个特定用户单独有一个组，他/她不属于其他任何组。个人组可以在 Group Name（组名）里用 @ 标识。个人组允许一个用户帐号有相同的组权限。

除了系统提供的上述默认组，您也可以根据需要创建组，给他们指定适当的权限。参看用户管理，了解如何创建和编辑用户组。

用户和组之间的关系

用户属于组，组有权限。将 KX II-101 的各种用户分成组，您可以同时管理一个组里所有用户的权限，而不用逐个用户管理权限，从而可以节省时间。

您还可以选择不让特定用户与组关联。在此情况下，可以把该用户归类为 Individual（个人）。

在成功验证之后，设备用组信息确定用户权限 — 可以访问哪些服务器端口，是否允许重新引导设备，以及其他功能。

用户管理

用户管理菜单

User Management（用户管理）菜单按下列方式组织管理：

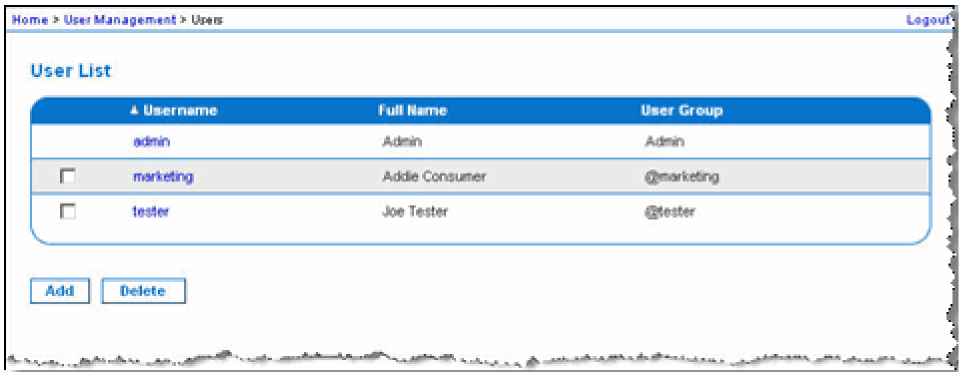
使用：	目的：
User List（用户列表）	显示所有用户的字母顺序列表；添加、修改或删除用户。
Add New User（添加新用户）	添加新用户；修改用户信息。
User Group List（用户组列表）	显示所有用户组的字母顺序列表；添加、修改或删除用户组。
Add New User Group（添加新用户组）	添加新用户组；修改用户组信息。
Change Password（更改密码）	更改特定用户的密码。
验证设置	配置用于访问 KX II-101 的验证的类型。

用户列表

User List（用户列表）页显示所有用户的列表，包括他们的用户名、全名和用户组。可以单击列名，按任意列排序列表。还可以在 User List（用户列表）页上添加、修改或删除用户。

➢ *查看用户列表：*

- 选择 User Management（用户管理）> User List（用户列表）。打开 User List（用户列表）页。



➢ *添加新用户：*

- 单击 Add（添加）按钮。打开 User（用户）页。如要了解有关用户页的完整信息，参看***添加新用户*** (p. 46)。

➢ *修改现有用户：*

1. 在列出的用户中找到要修改的用户。
2. 单击用户名。打开 User（用户）页。如要了解有关编辑用户的完整信息，参看***修改现有用户*** (p. 47)。

➢ *删除用户：*

1. 选择用户名左边的复选框，在列出的用户中选择要删除的用户。
2. 单击 Delete（删除）。系统提示您确认删除。
3. 单击 OK（确定）。

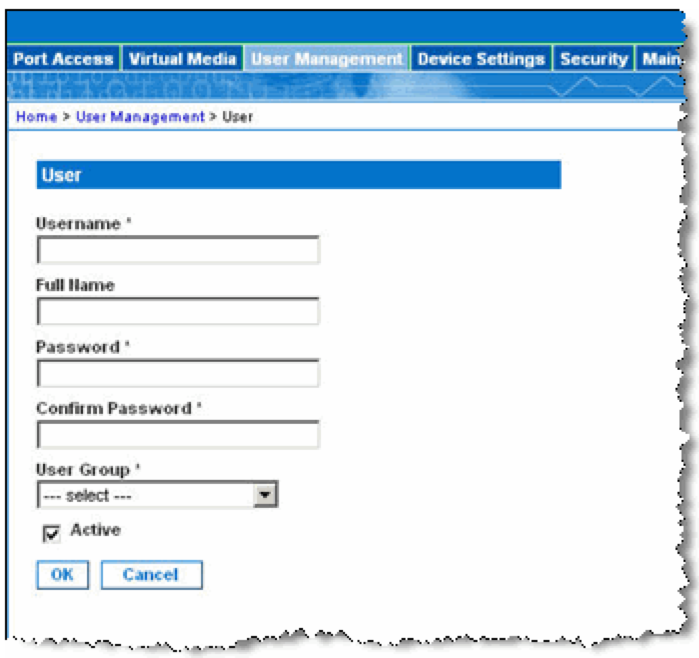
添加新用户

在创建 KX II-101 用户之前，最好先定义用户组，因为在添加用户时，必须给该用户指定一个现有用户组。可以在 User（用户）页上添加新用户，修改用户信息，重新激活已被停用的用户。

注意：可以停用用户名（当失败的登录尝试次数超过在 Security Settings [安全设置] 页上设置的最大登录尝试次数时，取消选择 Active [活动] 复选框）。参看安全设置了解详情。

➢ *添加新用户：*

1. 用下列方法之一打开 User（用户）页：
   - 选择 User Management（用户管理）> Add New User（添加新用户），或者
   - 单击 User List（用户列表）页上的 Add（添加）按钮



2. 在 Username（用户名）字段里输入一个唯一名称（最长 16 个字符）。
3. 在 Full Name（全名）字段里输入该用户的全名（最长 64 个字符）。
4. 在 Password（密码）字段里输入密码，在 Confirm Password（确认密码）字段里重新输入密码（最长 64 个字符）。

5. 在 User Group（用户组）下拉列表上选择组。除了系统提供的默认组（<Unknown [未知]>[默认值]、Admin [管理员] 和 Individual Group [个人组]），此列表还包含您创建的所有组。如果您不想使此用户与现有 User Group（用户组）关联，在 Individual Group（个人组）下拉列表上选择个人组。

   注意：管理员用户必须是管理员组的成员。

   如要详细了解个人组的权限，参看***设置个人组权限*** (p. 50)。
6. 如要激活此用户，选择 Active（活动）复选框。默认值是 activated（已激活，启用）。
7. 单击 OK（确定）。

修改现有用户

➢ *修改现有用户：*

1. 在 User（用户）页上更改相应的字段。（参看***添加新用户*** (p. 46)，了解如何访问 User [用户]页。）
2. 单击 OK（确定）。

阻止和允许用户

管理员可以阻止用户访问系统，也可以由系统根据安全设置自动阻止用户。参看***用户阻止*** (p. 136)了解详情。被阻止的用户变成不活动用户，管理员可以解除封锁，让他/她再次成为活动用户。

➢ *阻止或允许用户：*

1. 选择 User Management（用户管理）> User（用户）。

   打开 User（用户）页。
2. 选择或取消选择 Active（活动）复选框。
   - 如果选择，用户变成活动用户，被授予 KX II-101 访问权。
   - 如果取消选择，用户变成不活动用户，不能访问 KX II-101。
3. 单击 OK（确定）。

   用户的活动状态被更新了。

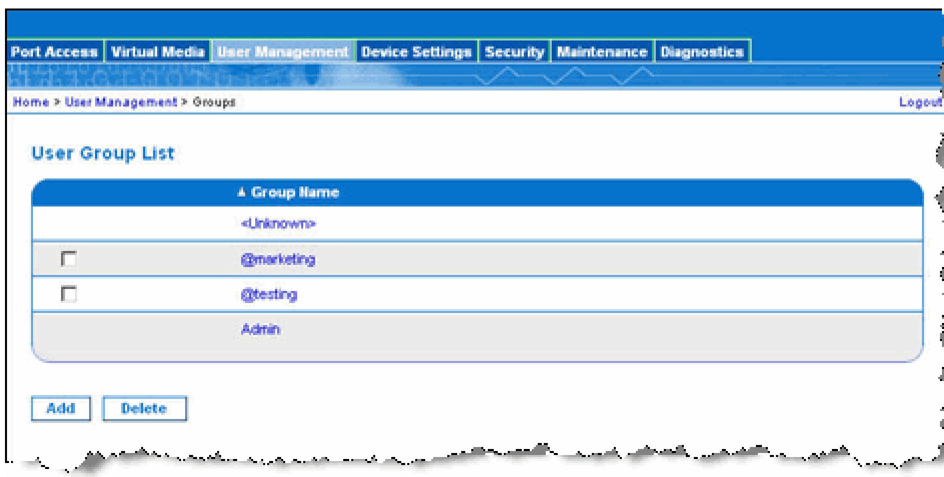
用户组列表

用户组用来进行本地和远程验证（通过 RADIUS 或 LDAP/LDAPS）。在创建个人用户之前，最好先定义用户组，因为在添加用户时，必须给该用户指定一个现有用户组。

User Group List（用户组列表）页显示所有用户组的列表，单击 Group Name（组名）列标题，即可按升序或降序排序列表。还可以在 User Group List（用户组列表）页上添加、修改或删除用户组。

➢ *列出用户组：*

- 选择 User Management(用户管理)> User Group List(用户组列表)。打开 User Group List（用户组列表）页。



➢ *添加新用户组：*

- 单击 Add（添加）按钮。打开 Group（组）页。如要了解有关组页的完整信息，参看添加新用户组。

➢ *修改现有用户组：*

1. 在列出的用户组中找到要修改的用户组。
2. 单击 Group Name（组名）。打开 Group（组）页。如要了解有关编辑组的完整信息，参看***修改现有用户组*** (p. 53)。

➢ *删除用户组：*

重要事项：如果删除有用户的组，自动给这些用户指定 <unknown（未知）>用户组。

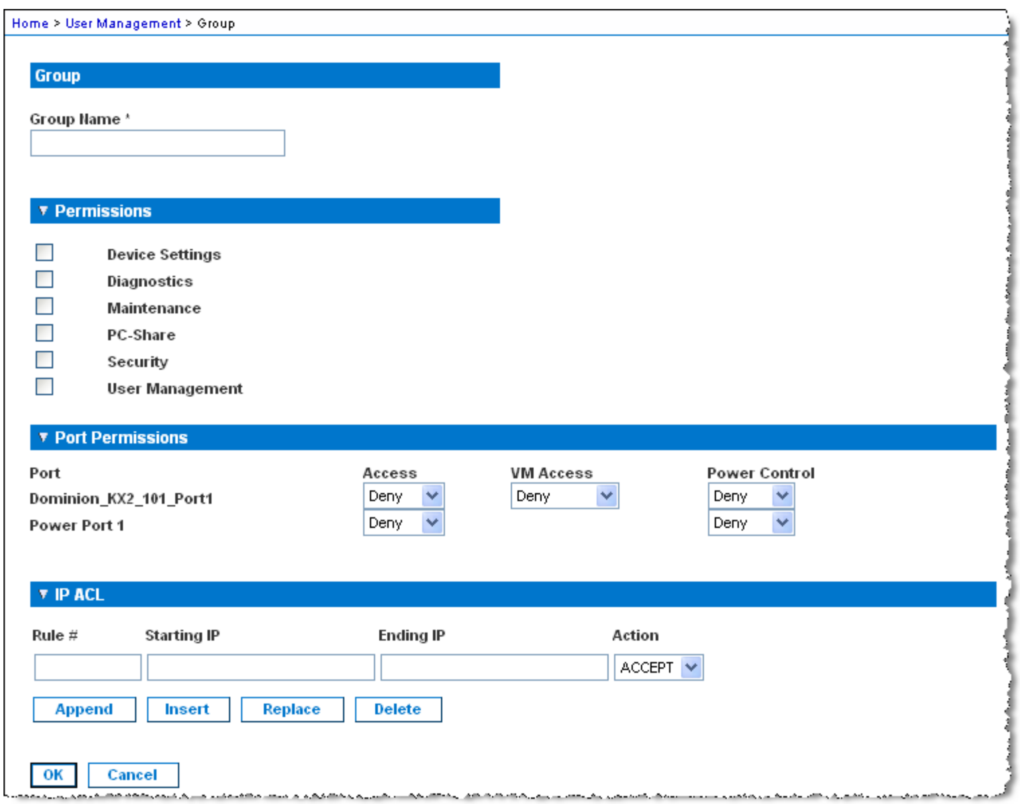
提示：如要确定属于特定组的用户，可以按 User Group（用户组）排序 User List（用户列表）。

1. 选择 Group Name（组名）左边的复选框，在列出的组中选择要删除的组。
2. 单击 Delete（删除）。
3. 在系统提示您确认删除时，单击 OK（确定）。

添加新用户组

➢ *添加新用户组：*

1. 用下列方法之一打开 Group（组）页：
   - 选择 User Management（用户管理）> Add New User Group（添加新用户组），或者
   - 单击 User Group List（用户组列表）页上的 Add（添加）按钮。



Group（组）页由下列几大类组成：Group（组）、Permissions（权限）、Port Permissions（端口权限）和 IP ACL。

2. 在 Group Name（组名）字段里输入新用户组的说明性名称。

3. 给该组设置 Permissions（权限）。选择要给该组所有用户指定的权限前面的复选框。参看***设置权限*** (p. 50)了解详情。
4. 设置 Port Permissions（端口权限）。指定 KVM 访问类型和电源端口。参看设置端口权限了解详情。
5. 设置 IP ACL（可选）。此功能通过指定 IP 地址来限制对 KX II-101 设备的访问；此功能仅适用于属于特定组的用户，不同于 ***IP 访问控制*** (p. 139)表功能，后者适用于尝试对该设备进行的所有访问（和优先级）。
6. 单击 OK（确定）。

注意：MPC 有几个管理功能可以使用；这些功能仅供默认 ADMIN（管理员）组的成员使用。

设置权限

重要事项：选择 User Management（用户管理）复选框，允许组成员更改所有用户的权限，包括他们自己的权限。授予这些权限时要仔细斟酌。

权限	说明
Device Settings（设备设置）	网络设置、日期/时间设置、端口配置（通道名称和电源关联）、事件管理 (SNMP 和 Syslog)、虚拟介质文件服务器设置。
Diagnostics（诊断）	网络接口状态、网络统计信息、ping 主机、跟踪到主机的路由、KX II-101 诊断。
Maintenance（维护）	备份和恢复数据库、固件升级、工厂复位、重新引导。
PC-Share（PC 共享）	多个用户同时访问同一个目标。
Security（安全性）	SSL 证书、安全设置（VM 共享和 PC 共享）、IP ACL。
User Management（用户管理）	用户和组管理、远程验证 (LDAP/RADIUS)、登录设置。

设置个人组权限

➢ *设置个人用户组权限：*

1. 在列出的组中找到该用户。个人组可以在 Group Name（组名）里用 @ 标识。
2. 单击 Group Name（组名）。打开 Group（组）页。
3. 选择适当的权限。
4. 单击 OK（确定）。

设置端口权限

对于服务器端口，可以指定访问类型、虚拟介质访问类型和电源控制。请注意所有权限的默认设置均将禁用。

访问		VM 访问		电源控制	
选项	说明	选项	说明	选项	说明
None（无）*	完全拒绝访问	Deny（拒绝）*	完全拒绝端口的虚拟介质权限	Deny（拒绝）*	完全拒绝访问
View（查看）	查看视频（但不与所连接的目标服务器交互操作）	Deny（拒绝）*	完全拒绝端口的虚拟介质权限	Deny（拒绝）*	完全拒绝访问
Control（控制）	控制所连接的目标服务器	虚拟介质访问仅限于只读访问	只读。虚拟介质全访问（读写）	Access（访问）	全访问
Control（控制）	控制所连接的目标服务器	Read-Write（读写）	虚拟介质全访问（读写）	Access or Deny（访问或拒绝）	全访问或完全拒绝访问

* 默认设置

基于组的 IP ACL（访问控制表）

重要事项：在使用基于组的 IP 访问控制时，务必小心谨慎。假如您的 IP 地址位于已拒绝访问的 IP 范围内，可能不能访问 KX II-101。

此功能限制所选组里使用特定 IP 地址的用户访问 KX II-101 设备。此功能仅适用于属于特定组的用户，它将被优先处理，不同于适用于对所有设备访问的 IP 访问控制表功能。参看 ***IP 访问控制*** (p. 139)了解详情。

使用 Group（组）页上的 IP ACL 部分，根据组级别添加、插入、替换和删除 IP 访问控制规则。



➢ *添加（附加）规则：*

1. 在 Starting IP（起始 IP）字段里输入起始 IP 地址。
2. 在 Ending IP（结束 IP）字段里输入结束 IP 地址。

3. 在可用的选项中选择 Action（操作）：
   - Accept(接受)。指定了 accept 的 IP 地址可以访问 KX II-101 设备。
   - Drop（放弃）。指定了 drop 的 IP 地址不能访问 KX II-101 设备。
4. 单击 Append（附加）。规则被添加到规则列表的底部。
5. 对于要输入的每个规则，重复步骤 1 到步骤 4。

➢ *插入规则:*

1. 输入 Rule #(规则号)。在使用 Insert(插入)命令时，需要填写 Rule #（规则号）。
2. 在 Starting IP（起始 IP）和 Ending IP（结束 IP）字段里输入 IP 地址。
3. 在 Action（操作）下拉列表上选择操作。
4. 单击 Insert（插入）。如果刚才输入的 Rule #（规则号）与现有 Rule #（规则号），新规则将放在现有规则的前面，列表上的所有规则均向下移动。

➢ *替换规则:*

1. 指定要替换的 Rule #（规则号）。
2. 在 Starting IP（起始 IP）和 Ending IP（结束 IP）字段里输入 IP 地址。
3. 在 Action（操作）下拉列表上选择操作。
4. 单击 Replace（替换）。新规则替换有相同 Rule #（规则号）的原始规则。

➢ *删除规则:*

1. 指定要删除的 Rule #（规则号）。
2. 单击 Delete（删除）。
3. 在系统提示您确认删除时，单击 OK（确定）。

重要事项：根据 ACL 规则的列出顺序对这些规则进行求值。例如在此示例中，如果两个 ACL 规则颠倒了，Dominion 可能不接受任何通信。



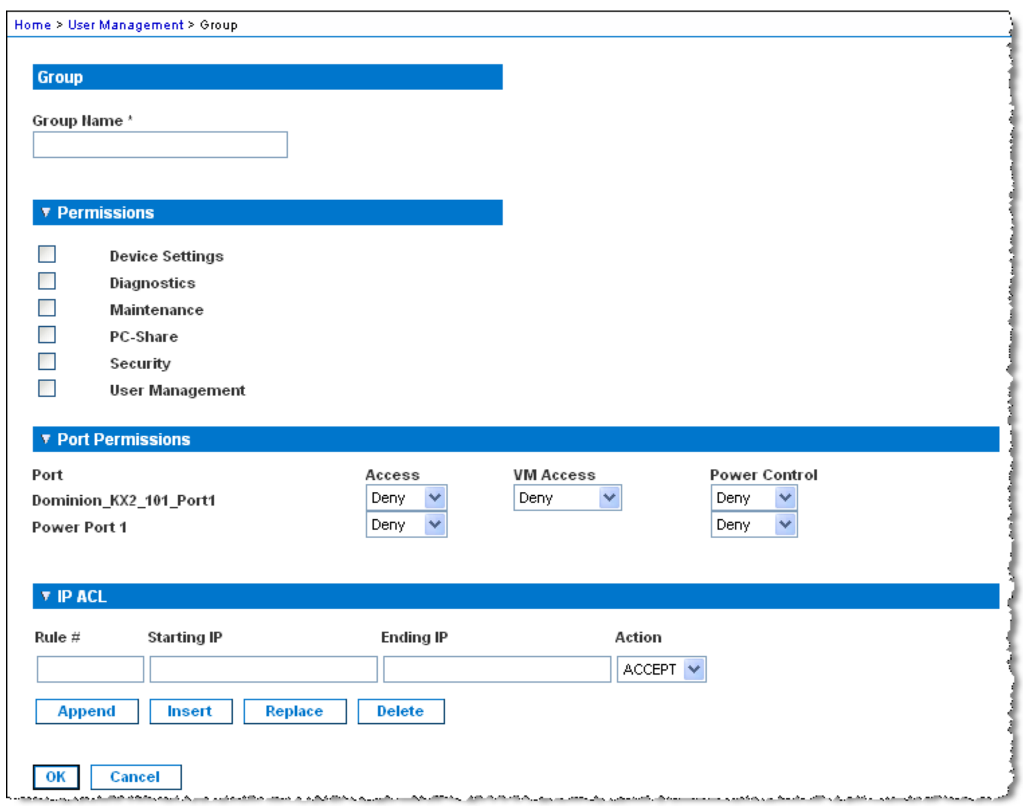
提示：规则号便于您更好地控制规则创建顺序。

修改现有用户组

注意：启用 Admin（管理员）组的所有权限。

➢ *修改现有用户组：*

1. 在 Group（组）页上更改相应的字段，设置适当的权限。



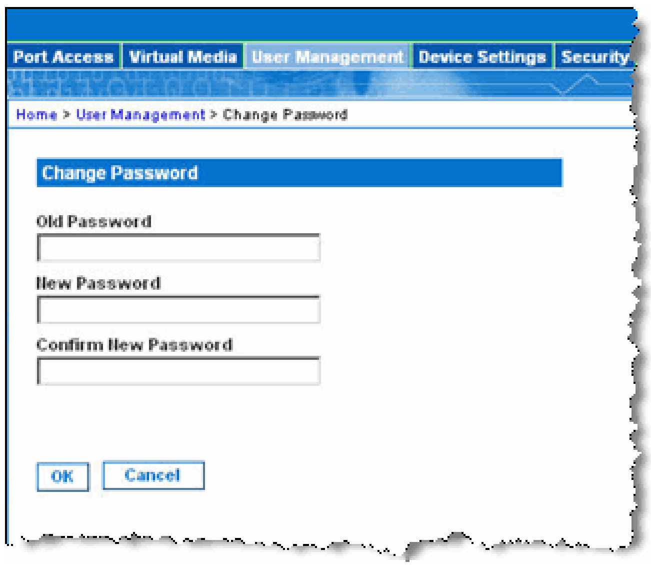
2. 给该组设置 Permissions（权限）。选择要给此组所有用户指定的权限前面的复选框。参看 ***设置权限*** (p. 50) 了解详情。

3. 设置 Port Permissions（端口权限）。指定此组的用户可以访问的服务器端口（和访问类型）。参看设置端口权限了解详情。
4. 设置 IP ACL（可选）。此功能通过指定 IP 地址来限制 KX II-101 设备访问。参看基于组的 IP 访问控制表了解详情。
5. 单击 OK（确定）。

更改密码

➢ *更改密码:*

1. 选择 User Management（用户管理）> Change Password（更改密码）。打开 Change Password（更改密码）页。



2. 在 Old Password（旧密码）字段里输入当前密码。
3. 在 New Password（新密码）字段里输入新密码，在 Confirm New Password（确认新密码）字段里重新输入新密码。密码最长可达 64 个字符，可以由英文字母数字字符和特殊字符组成。
4. 单击 OK（确定）。
5. 将显示确认信息，说明密码更改成功。单击 OK（确定）。

---

*注意：如果使用强密码，本页显示有关这种密码所要求格式的信息。如要详细了解密码和强密码，参看*安全设置 — 强密码 *(参看 "强密码" p. 135)。*

验证设置

本章后面的远程验证部分将讨论验证设置。参看验证设置了解详情。

远程验证

CC-SG 用户注意事项

在用 CommandCenter Secure Gateway 控制 KX II-101 时，除了（需要本地端口访问的）本地用户，CC-SG 要验证用户和组。当 CC-SG 控制 KX II-101 时，将根据在 KX II-101 上配置的本地用户数据库或 Remote Authentication server (LDAP/LDAPS or RADIUS) 验证本地端口用户，而不根据 CC-SG 用户数据库验证这些用户。

如要进一步了解 CC-SG 验证，参看下列网址上的《CommandCenter Secure Gateway 用户指南》、《管理员指南》或《部署指南》：***http://www.raritan.com/support/*** http://www.raritan.com/support。

支持的协议

为了简化用户名和密码管理，KX II-101 可以将验证请求转发到外部验证服务器。支持两种外部验证协议：LDAP/LDAPS 和 RADIUS。

有关 Microsoft Active Directory 的说明

Microsoft Active Directory 使用本机 LDAP 协议，可以充当 LDAP 服务器和 KX II-101 验证源。如果 Microsoft Active Directory 服务器有 IAS (Internet Authorization Server) 组件，它还可以作为 RADIUS 验证源。

验证和授权

验证是确定用户真实身份这一过程。一旦一个用户经过验证，就用该用户的组确定他/她的系统权限和端口权限。给用户指定的权限决定了允许的访问类型。这叫做授权。

如果配置 KX II-101 进行远程验证，外部验证服务器主要用于验证，而不是授权。

验证设置

可以在 Authentication Settings（验证设置）页上配置用于访问 KX II-101 的验证类型。参看***验证和授权*** (p. 55)，了解验证和授权的工作原理，以及二者的区别。

注意：即使选择远程验证（LDAP 或 RADIUS），仍然要使用本地验证。

➢ *配置验证：*

1. 选择 User Management（用户管理）> Authentication Settings（验证设置）。打开 Authentication Settings（验证设置）页：



2. 选择要使用的验证协议选项（Local Authentication [本地验证]、LDAP 或 RADIUS）。如果选择 LDAP 选项，将启用其余的 LDAP 字段；如果选择 RADIUS 选项，将启用其余的 RADIUS 字段。

3. 如果选择 Local Authentication（本地验证），继续到步骤 6。

4. 如果选择 LDAP，参看实现 LDAP 远程验证一节，了解如何填写 Authentication Settings（验证设置）页上 LDAP 部分的字段。
5. 如果选择 RADIUS，参看***实现 RADIUS 远程验证*** (p. 61)一节，了解如何填写 Authentication Settings（验证设置）页上 RADIUS 部分的字段。
6. 单击 OK（确定）按钮保存设置。

➢ *取消而不保存更改：*

- 单击 Cancel（取消）。

➢ *恢复到出厂默认值：*

- 单击 Reset to Defaults（恢复默认值）按钮。

实现 LDAP 远程验证

Lightweight Directory Access Protocol (LDAP) 是用于查询和修改基于 TCP/IP 运行的目录服务的网络协议。客户机连接 LDAP 服务器（默认 TCP 端口是 389），启动 LDAP 会话。客户机向服务器发送操作请求，服务器返回响应。

提示：Microsoft Active Directory 在本机充当 LDAP 验证服务器。

➢ *如要使用 LDAP 验证协议，输入下列信息：*



1. 在 Primary LDAP Server（主 LDAP 服务器）字段里输入 LDAP 远程验证服务器的 IP 地址或 DNS 名称。如果选择了 Enable Secure LDAP（启用安全 LDAP）选项，必须使用 DNS 名称。

2. （可选）在 Secondary LDAP Server（备用 LDAP 服务器）字段里输入备用 LDAP 服务器的 IP 地址或 DNS 名称。如果选择了 Enable Secure LDAP（启用安全 LDAP）选项，必须使用 DNS 名称。请注意其余字段共享 Primary LDAP Server（主 LDAP 服务器）字段的设置。
3. 在 Secret Phrase（密码）字段里输入利用远程验证服务器进行验证所需的服务器密码，在 Confirm Secret Phrase（确认密码）字段里再次输入密码。不要更改现有验证模式。使用在 LDAP 服务器上所用的字符串。
4. 如果要使用 SSL，选择 Enable Secure LDAP（启用安全 LDAP）复选框，启用 Secure LDAP Port（安全 LDAP 端口）字段。Secure Sockets Layer (SSL) 加密协议允许 KX II-101 与 LDAP 服务器安全通信。
5. 默认端口是 389。使用标准 LDAP TCP 端口，或者指定另一个端口。
6. 默认 Secure LDAP Port（安全 LDAP 端口）是 636。使用默认端口，或者指定另一个端口。在选择 Enable Secure LDAP（启用安全 LDAP）复选框时，启用此字段。
7. 证书文件。咨询验证服务器管理员，获取 LDAP 服务器所用的 Base64 编码 X-509 格式的 CA 证书文件。用 Browse（浏览）按钮找到证书文件。在选择 Enable Secure LDAP（启用安全 LDAP）选项时，启用此字段。
8. 管理用户的 DN。管理用户的辨别名；咨询验证服务器管理员，了解要在此字段里输入的相应值。管理用户 DN 的值可能是这样的："cn=Administrator,cn=Users,dc=testradius,dc=com"。
9. 用户搜索 DN。它说明要与 LDAP 绑定在一起的名称，以及在数据库的什么地方开始搜索指定的 Base DN。Base Search（基本搜索）值可能是这样的："cn=Users,dc=raritan,dc=com"。咨询验证服务器管理员，了解要在这些字段里输入的相应值。
10. 外部 LDAP 服务器的类型。在可用选项中选择：
    - Generic LDAP Server（常规 LDAP 服务器）。
    - Microsoft Active Directory。Active Directory 是 Microsoft 实现的 LDAP 目录服务，在 Windows 环境下使用。
11. Active Directory Domain（Active Directory 域）。输入 Active Directory Domain（Active Directory 域）的名称。

从 Active Directory 服务器返回用户组信息

KX II-101 支持用户用 Active Directory (AD) 进行验证，不需要在 KX II-101 上本地定义这些用户。这样，Active Directory 用户帐号和密码只保存在 AD 服务器上。授权和 AD 用户权限通过标准 KX II-101 策略和用户组权限（本地应用于 AD 用户组）进行控制和管理。

*注意：如果您现在是 Raritan, Inc. 客户，而且已经通过更改 AD 模式配置了 Active Directory 服务器，KX II-101 仍然支持此配置，您不必执行下列操作。参看***更新 LDAP 模式** *(p. 63)，了解如何更新 AD LDAP 模式。*

➢ *在 KX II-101 上启用 AD 服务器：*

1. 用 KX II-101 创建特殊组，给这些组指定适当的权限。例如创建这样的组：KVM_Admin 和 KVM_Operator。
2. 在 Active Directory 服务器上创建与上一步创建的组同名的新组。
3. 在 AD 服务器上给 KX II-101 用户指定在步骤 2 中创建的组。
4. 在 KX II-101 上正确启用和配置 AD 服务器。参看实现 LDAP 远程验证。

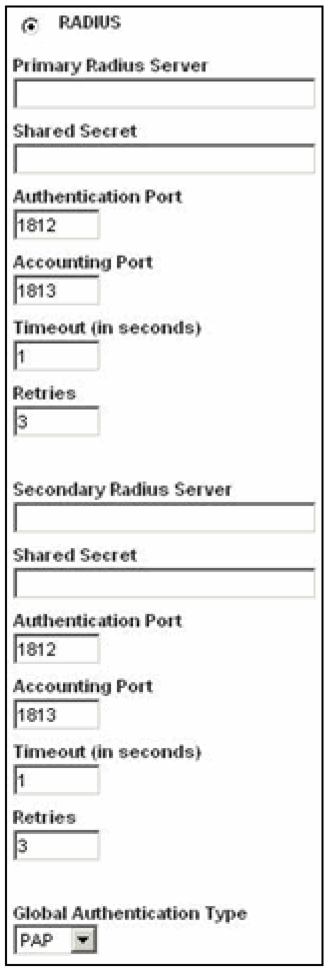
重要注意事项：

- 组名区分大小写。
- KX II-101 提供下列不能更改或删除的默认组：Admin（管理员）和 <Unknown（未知）>。请确认 Active Directory 服务器不使用相同的组名。
- 如果 Active Directory 服务器返回的组信息与 KX II-101 组配置不匹配，KX II-101 自动给成功验证的用户指定 <Unknown（未知）>组。

实现 RADIUS 远程验证

Remote Authentication Dial-in User Service (RADIUS) 是供网络访问应用程序使用的 AAA (authentication, authorization, and accounting) 协议。

➢ *使用 RADIUS 验证协议：*



1. 分别在 Primary Radius Server（主 Radius 服务器）和 Secondary Radius Server（备用 Radius 服务器）字段里输入主远程验证服务器和（可选）备用远程验证服务器的 IP 地址。
2. （在 Shared Secret [共享密码]字段里）输入用于验证的服务器密码。共享密码必须是 KX II-101 和 RADIUS 服务器都知道的字符串，这样它们才能进行安全通信。共享机密实质上就是密码。
3. Authentication Port（验证端口）。默认验证端口是 1812，可以按需要更改。

4. Accounting Port（记帐端口）。默认记帐端口是 1813，可以按需要更改。
5. Timeout (in seconds)（超时[秒]）。默认超时是 1 秒，可以按需要更改。超时是 KX II-101 在发送另一个验证请求之前，等待 RADIUS 服务器响应的时间。
6. Retries（再试次数）。默认再试次数是 3，可以按需要更改。这是 KX II-101 给 RADIUS 服务器发送验证请求的次数。
7. Global Authentication Type（全局验证类型）。在下拉列表上的选项中选择选项：
   - PAP。在选择 PAP 时，密码采用纯文本形式发送。PAP 不是交互式的；在建立连接之后，用户名和密码作为一个数据包发送，而不是服务器先发送登录提示，然后等待响应。
   - CHAP。在选择 CHAP 时，服务器随时可以请求验证。CHAP 的安全性比 PAP 高。

通过 RADIUS 返回用户组信息

在 RADIUS 验证尝试成功之后，KX II-101 设备根据用户组的权限确定给定用户的权限。

远程 RADIUS 服务器返回一个作为 RADIUS FILTER-ID 实现的属性，提供这些用户组名。FILTER-ID 的格式如下：

Raritan:G{GROUP_NAME}

其中 GROUP_NAME 是表示用户所属组的名称的字符串。

RADIUS 通信交换规范

KX II-101 设备给 RADIUS 服务器发送下列 RADIUS 属性：

属性	数据
登录	
Access-Request (1)	
NAS-Port-Type (61)	网络连接的 VIRTUAL (5)。
NAS-IP-Address (4)	KX II-101 设备的 IP 地址。
User-Name (1)	在登录屏幕上输入的用户名。
Acct-Session-ID (44)	用于记帐的会话 ID。
User-Password (2)	经过加密的密码。

属性	数据
登录	
Accounting-Request(4)	
Acct-Status (40)	Start(1) — 开始记帐。
NAS-Port-Type (61)	网络连接的 VIRTUAL (5)。
NAS-Port (5)	始终是 0。
NAS-IP-Address (4)	KX II-101 设备的 IP 地址。
User-Name (1)	在登录屏幕上输入的用户名。
Acct-Session-ID (44)	用于记帐的会话 ID。
注销	
Accounting-Request(4)	
Acct-Status (40)	Stop(2) — 停止记帐
NAS-Port-Type (61)	网络连接的 VIRTUAL (5)。
NAS-Port (5)	始终是 0。
NAS-IP-Address (4)	KX II-101 设备的 IP 地址。
User-Name (1)	在登录屏幕上输入的用户名。
Acct-Session-ID (44)	用于记帐的会话 ID。

更新 LDAP 模式

注意：本章介绍的步骤仅供有经验的用户使用。

返回用户组信息

一旦验证成功，就可以用本章中的信息返回用户组信息（需要相应的授权）。

从 LDAP 返回

在 LDAP/LDAPS 验证成功之后，KX II-101 根据给定用户所在组的权限确定该用户的权限。远程 LDAP 服务器可以返回如下属性，提供这些用户组名称：

rciusergroup attribute type: string

这可能要求 LDAP 服务器有模式扩展。咨询验证服务器管理员，了解如何启用此属性。

从 Microsoft Active Directory 返回

注意：仅供有经验的 Active Directory 管理员使用。

从 Windows 2000 Server 服务器上的 Microsoft Active Directory 返回用户组信息，需要更新 LDAP/LDAPS 模式。参看 Microsoft 文档了解详情。

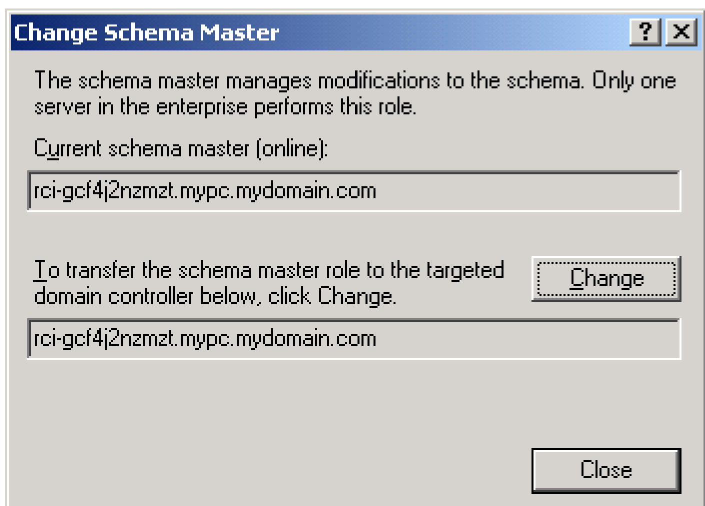
1. 安装 Active Directory 模式插件 — 参看 Microsoft Active Directory 文档了解安装说明。
2. 运行 Active Directory 控制台，选择 Active Directory Schema（Active Directory 模式）。

设置注册表启用模式写入操作

为了让域控制器写入模式，必须设置注册表项，允许模式更新。

➢ *启用模式写入操作：*

1. 用右键单击窗口左窗格上的 Active Directory Schema（Active Directory 模式）根节点，然后单击 Operations Master（操作主控）。打开 Change Schema Master（更改模式主控）对话框。

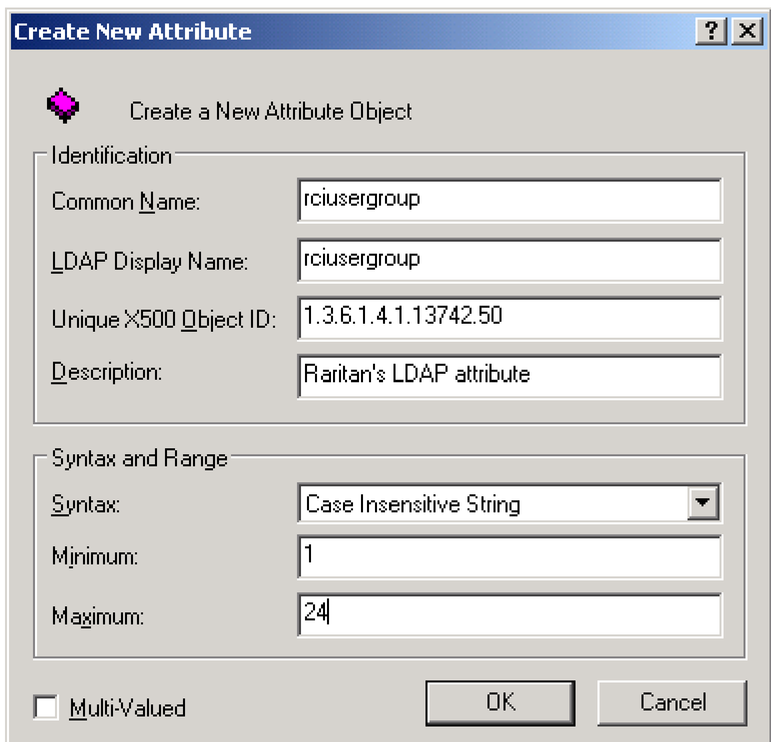


2. （可选）选择 The Schema may be modified on this Domain Controller（可以在此域控制器上修改模式）前面的复选框。
3. 单击 OK（确定）。

创建新属性

➢ *给 rciusergroup 类创建新属性:*

1. 单击窗口左窗格上 Active Directory Schema（Active Directory 模式）前面的 + 号。
2. 用右键单击左窗格上的 Attributes（属性）。
3. 单击 New（新建），然后选择 Attribute（属性）。在显示警告消息时，单击 Continue（继续）按钮，打开 Create New Attribute（创建新属性）对话框。



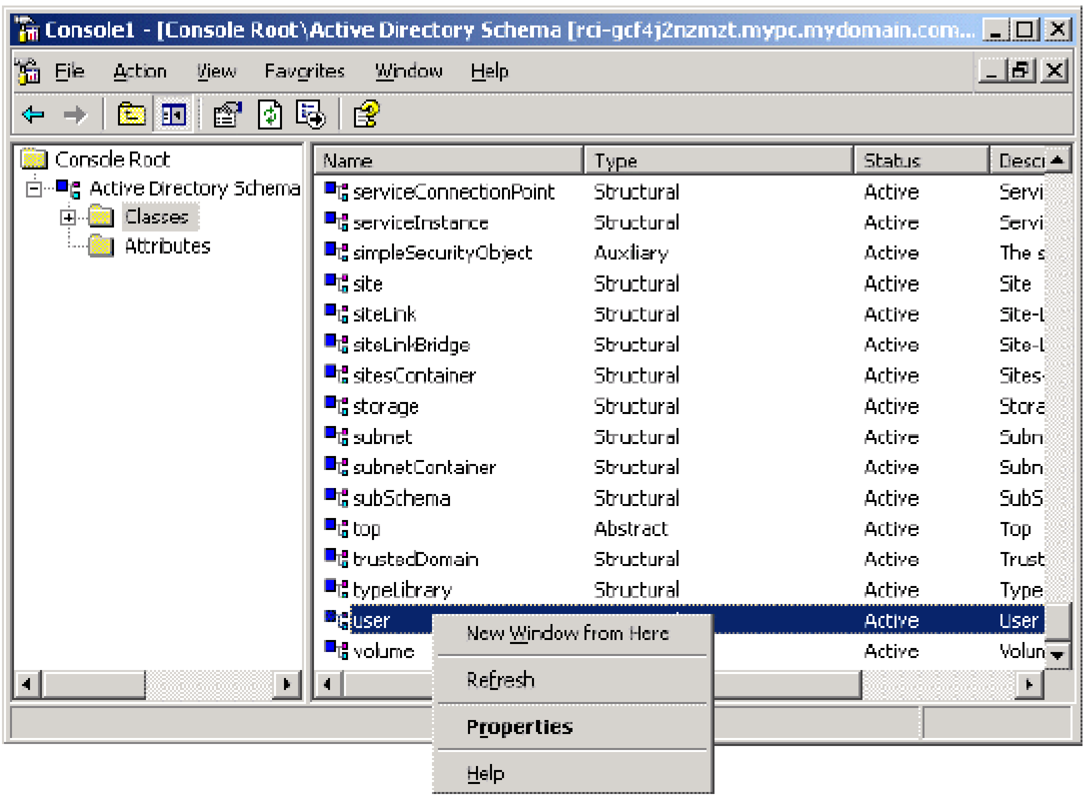
4. 在 Common Name（通用名称）字段里输入 *rciusergroup*。
5. 在 LDAP Display Name（LDAP 显示名称）字段里输入 *rciusergroup*。
6. 在 Unique x5000 Object ID（唯一 x5000 对象 ID）字段里输入 *1.3.6.1.4.1.13742.50*。
7. 在 Description（说明）字段里输入有意义的说明。
8. 单击 Syntax（语法）下拉箭头，在列表上选择 Case Insensitive String（不区分大小写的字符串）。
9. 在 Minimum（最小值）字段里输入 *1*。

10. 在 Maximum（最大值）字段里输入 *24*。
11. 单击 OK（确定）按钮创建新属性。

给类添加属性

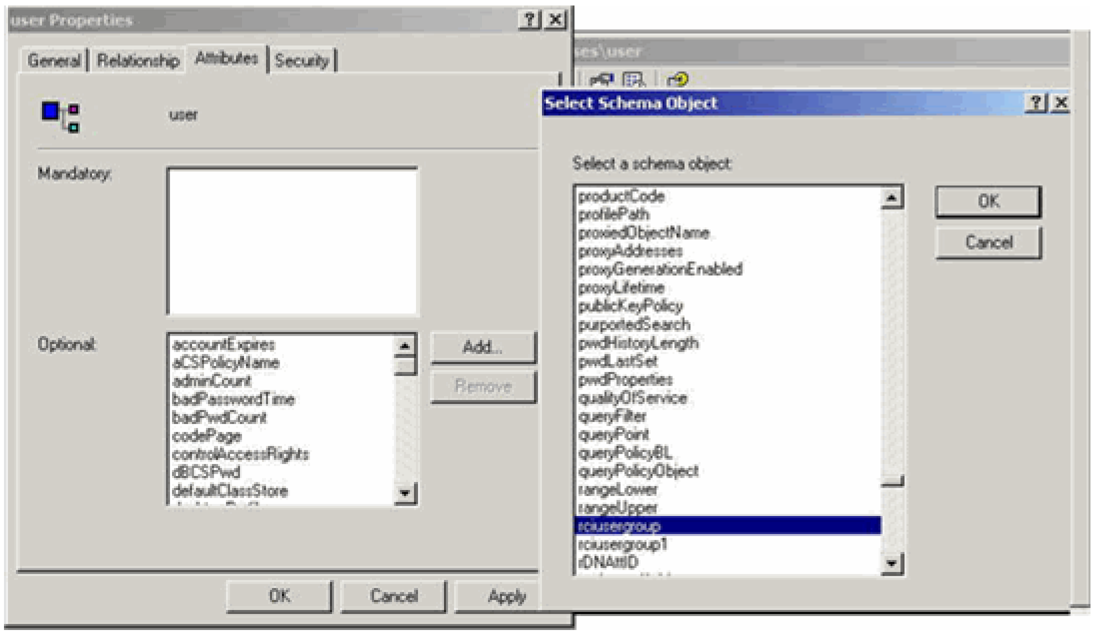
➤ *给类添加属性：*

1. 单击窗口左窗格上的 Classes（类）。
2. 滚动右窗格上的 user（用户）类，用右键单击它。



3. 在菜单上选择 Properties（属性）。打开 User Properties（用户属性）窗口。

4. 单击并打开 Attributes（属性）选项卡。



5. 单击 Add（添加）。
6. 在 Select Schema Object（选择模式对象）列表上选择 rciusergroup。
7. 单击 Select Schema Object（选择模式对象）对话框上的 OK（确定）。
8. 单击 User Properties（用户属性）对话框上的 OK（确定）。

更新模式高速缓存

➢ *更新模式高速缓存：*

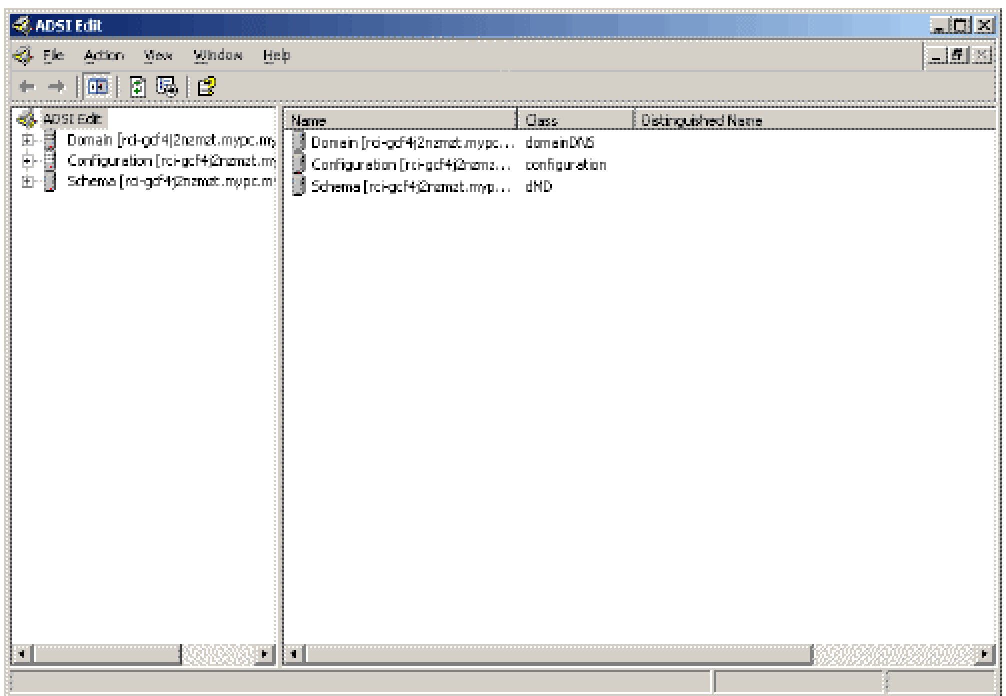
1. 用右键单击窗口左窗格上的 Active Directory Schema（Active Directory 模式），在快捷菜单上选择 Reload the Schema（重新加载模式）。
2. 最小化 Active Directory Schema（Active Directory 模式）MMC (Microsoft Management Console) 控制台。

编辑用户成员的 rciusergroup 属性

如要在 Windows 2003 服务器上运行 Active Directory 脚本，使用 Microsoft 提供的脚本（可以在 Windows 2003 服务器安装 CD 上找到）。可以用 Microsoft Windows 2003 安装 CD 把这些脚本加载到系统里。ADSI (Active Directory Service Interface) 充当 Active Directory 低级别编辑器，便于您用目录服务执行一些常见管理任务，例如添加、删除和移动对象。

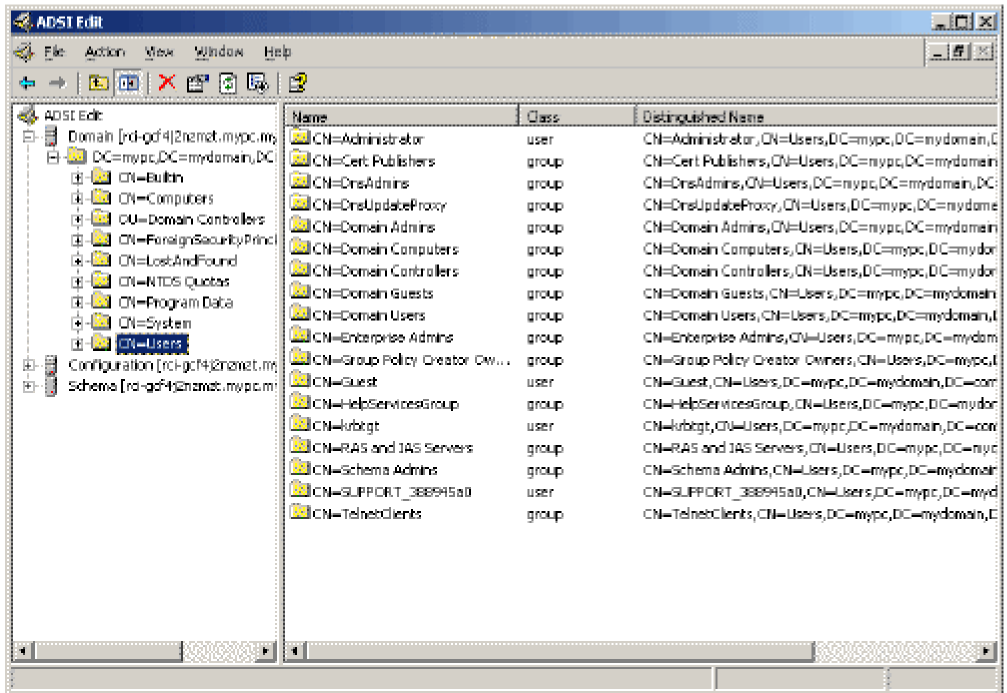
➢ *编辑组 rciusergroup 里的个人用户属性：*

1. 在安装 CD 上选择 Support（支持）> Tools（工具）。
2. 双击 SUPTOOLS.MSI 安装支持工具。
3. 找到支持工具安装目录。
4. 运行 adsiedit.msc。打开 ADSI Edit（ADSI 编辑）窗口。



5. 打开 Domain（域）。

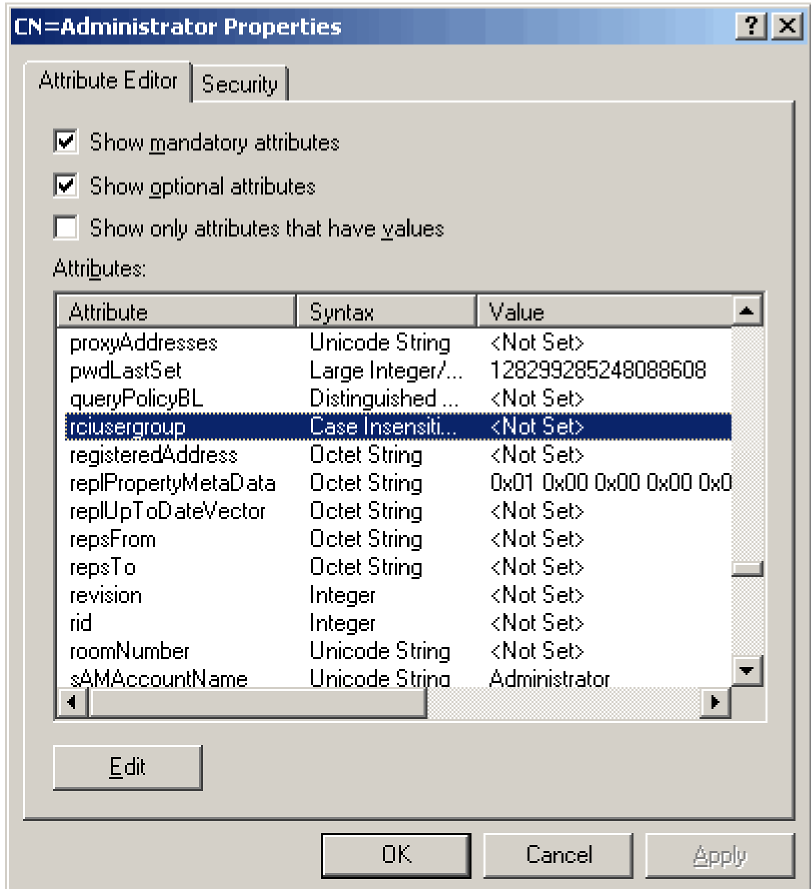
6. 在窗口左窗格上选择 CN=User 文件夹。



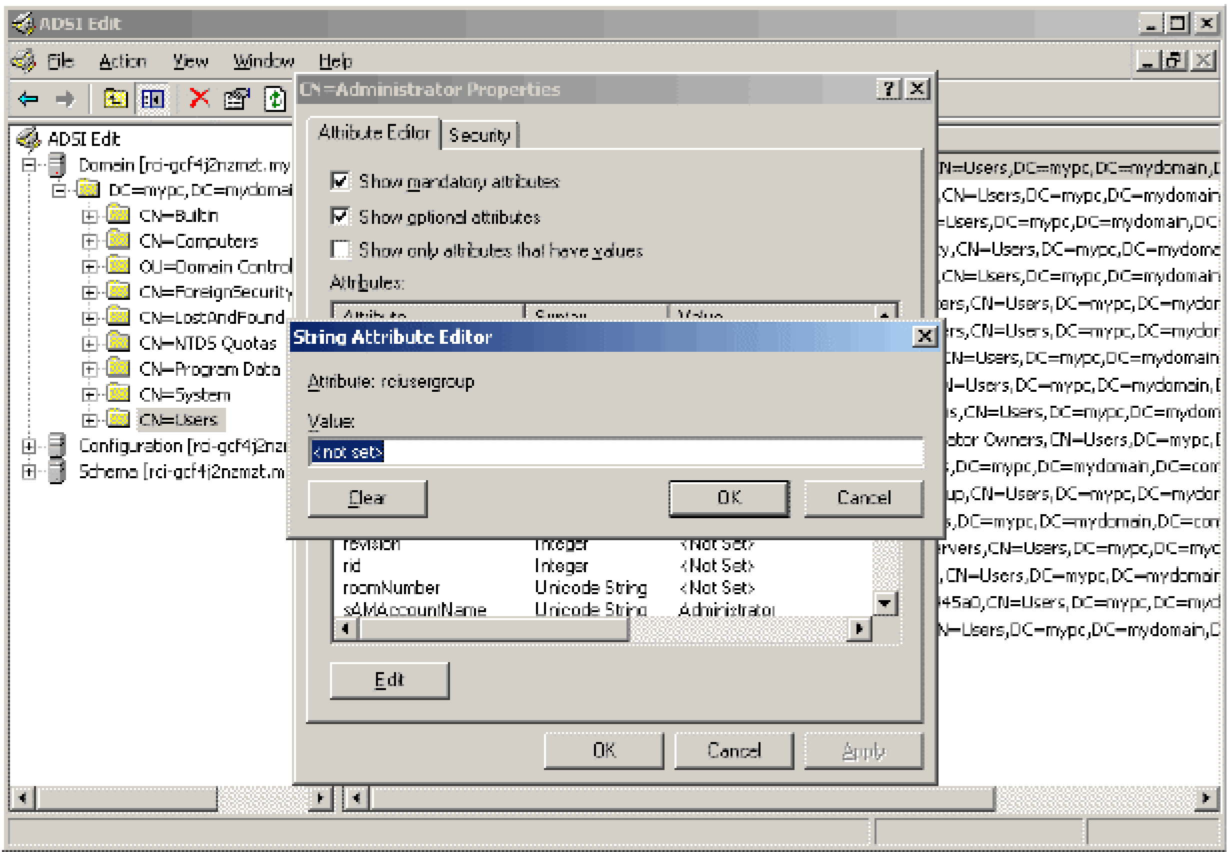
7. 在右窗格上找到要调整其属性的用户名。用右键单击用户名，选择 Properties（属性）。

8. 如果打不开，单击 Attributes（属性）选项卡。

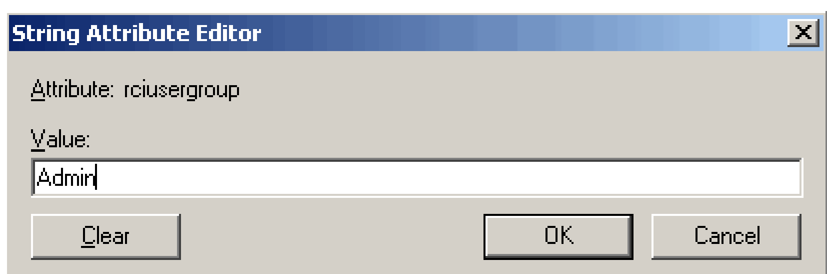
9. 在 Attributes（属性）列表上选择 rciusergroup。



10. 单击 Edit（编辑）。打开 String Attribute Editor（字符串属性编辑器）对话框。



11. 在 Edit Attribute（编辑属性）字段里输入（在 Dominion KX II-101 里创建的）用户组。



12. 单击 OK（确定）。

6 Virtual KVM Client

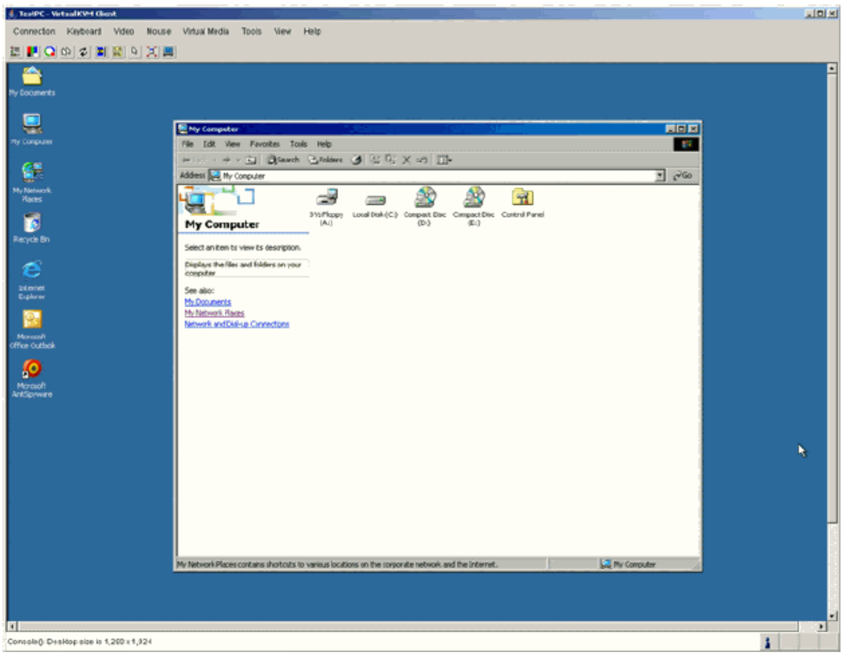
在本章内

概述

每当用 KX II-101 Remote Console 访问目标服务器时，都打开 Virtual KVM Client 窗口。

Virtual KVM Client 窗口可以最小化和最大化，可以在计算机桌面上移动。

注意：在刷新 HTML 浏览器时，会关闭 Virtual KVM Client 连接，所以要谨慎。



Virtual KVM Client 的功能可通过菜单和工具栏访问。

功能	说明
菜单栏	命令和设置的下拉菜单。
工具栏	常用功能和命令的快捷按钮。
目标服务器视频窗口	目标设备显示。
状态栏	有关连接参数、目标服务器窗口大小、并发连接、Caps Lock 指示器和 Num Lock 指示器的实时信息。

选项

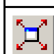
菜单树

下表列出 Virtual KVM Client 的所有菜单和菜单项。

- Connection（连接）菜单：
  - Properties（属性）
  - Connection Info（连接信息）
  - Exit（退出）
- Keyboard（键盘）菜单：
  - Send Ctrl + Alt + Delete（发送 Ctrl + Alt + Delete）
  - Keyboard Macros（键盘宏）
  - Keyboard Mouse Options（键盘鼠标选项）
  - User-Created Macros **Optional**（自定义宏[可选]）
- Video（视频）菜单
  - Refresh Screen（刷新屏幕）
  - Auto-Sense Video Settings（自动检测视频设置）
  - Calibrate Color（校准色彩）
  - Video Settings（视频设置）
- Mouse（鼠标）菜单：
  - Synchronize Mouse（同步鼠标）
  - Single Mouse Cursor（单鼠标光标）
  - Absolute（绝对）
  - Intelligent（智能）
  - Standard（标准）
- Virtual Media（虚拟介质）菜单：
  - Connect Drive（连接驱动器）
  - Connect CD-ROM/ISO Image（连接 CD-ROM/ISO 映像）
- Tools（工具）菜单：
  - Options（选项）
- View（视图）菜单：
  - View Toolbar（视图工具栏）
  - Scaling（缩放）

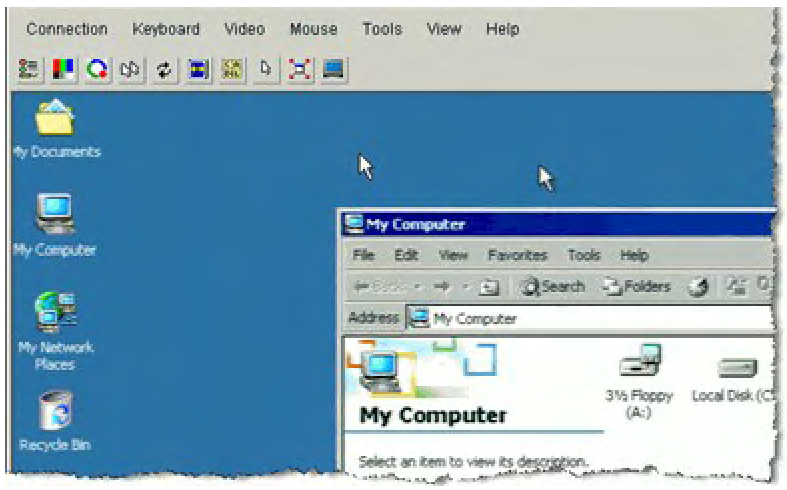
- Target Screen Resolution（目标屏幕分辨率）
- Help（帮助）菜单：
  - About Raritan Virtual KVM Client（关于 Raritan Virtual KVM Client）

工具栏

按钮	说明
	Properties（属性）
	Video settings（视频设置）
	Calibrate color（校准色彩）
	Synchronize the target mouse cursor(同步目标鼠标光标）
	Refresh screen（刷新屏幕）
	Auto-sense video（自动检测视频）
	Send Ctrl+Alt+Delete（发送 Ctrl+Alt+Delete）
	Single Mouse Cursor（单鼠标光标）
	Full screen（全屏）
	Resize video to fit screen（调整视频大小以适合屏幕）

Mouse Pointer Synchronization（鼠标指针同步）

在远程查看使用鼠标的目标服务器时，您会看到两个鼠标指针：一个是远程客户机工作站的，另一个是目标服务器的。当鼠标指针位于 Virtual KVM Client 目标服务器窗口之内时，鼠标移动和单击操作被直接传输到相连的目标服务器。由于鼠标加速度设置的缘故，客户机鼠标指针在移动过程中会稍微领先于目标服务器鼠标指针。



在快速 LAN 连接上，可能要禁用 Virtual KVM Client 鼠标指针，只看到目标服务器指针。可以在这两种模式（单鼠标和双鼠标）之间切换。参看***鼠标菜单*** (p. 88)进一步了解可用的鼠标模式。

鼠标同步提示

在进行鼠标同步时，切记遵循下列步骤：

1. 确定所选的视频分辨率和刷新速率是 KX II-101 设备支持的分辨率和刷新速率。Virtual KVM Client Connection Info（Virtual KVM Client 连接信息）对话框显示 KX II-101 设备看到的实际值。参看设备用户指南上的支持的视频分辨率部分，了解支持的视频分辨率。
2. 确定电缆长度是否在所选的视频分辨率允许的指定范围内。参看设备用户指南上的目标服务器连接距离和视频分辨率部分了解详情。
3. 确定在安装过程中是否正确配置了鼠标和视频。参看设备用户指南上的安装和配置部分，了解完整说明。
4. 单击 Auto-sense Video Settings（自动检测视频设置）按钮，执行自动检测。
5. 如果这不能提高（Linux、UNIX 和 Solaris KVM 目标服务器的）鼠标同步效果：
    a. 打开终端窗口。

b. 输入 *xset mouse 1 1* 命令。

c. 关闭终端窗口。

6. 单击 Virtual KVM Client 鼠标同步按钮。

其他智能鼠标模式说明

- 切记屏幕左上角没有图标或应用程序，因为那是同步例程运行的地方。
- 不要使用动画鼠标。
- 在目标服务器上禁用活动桌面。

连接菜单

属性对话框

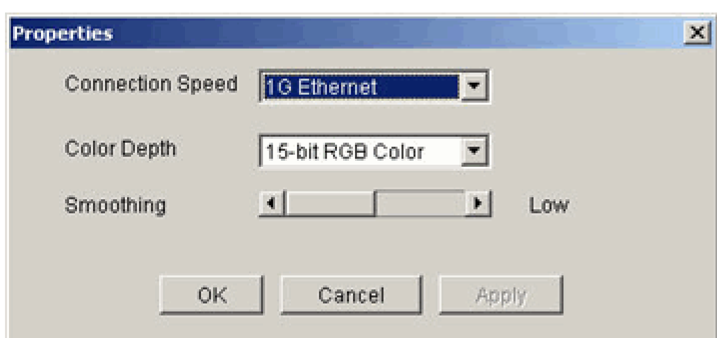
KX II-101 动态视频压缩算法保证在带宽约束不断变化的条件下，KVM 控制台的可用性。KX II-101 设备不仅针对 LAN 优化 KVM 输出，还针对 WAN 优化 KVM 输出。这些设备还能控制色彩深度并限制视频输出，无论在什么带宽条件下，均能在视频质量和系统响应之间实现最佳平衡。

	Connection Properties（连接属性）	人工调整与带宽有关的选项（连接速度、色彩深度等）。

对于不同的操作环境，可以根据需要优化 Properties（属性）对话框上的参数。

➢ *设置连接属性：*

1. 选择 Connection（连接）> Properties（属性）。打开 **Properties（属性）**对话框。



2. 在 Connection Speed（连接速度）下拉列表上选择连接速度。KX II-101 可以自动检测可用带宽，不限制带宽使用，但您也可以根据带宽限制调整使用情况。

Auto（自动）

1G Ethernet

100 Mb Ethernet

10 Mb Ethernet

1.5 Mb (MAX DSL/T1)

1 Mb (Fast DSL/T1)（1 Mb [快速 DSL/T1]）

512 Kb (Medium DSL/T1)（512 Kb [中速 DSL/T1]）

384 Kb (Slow DSL/T1)（384 Kb [低速 DSL/T1]）

256 Kb (Cable)（256 Kb [电缆]）

128 Kb (Dual ISDN)（128 Kb [双 ISDN]）

请注意这些设置是特定条件下的最佳值，而不是精确速度。无论当前网络速度和编码设置如何，客户机和服务器始终尝试尽快通过网络传输视频。但如果设置与真实环境吻合，系统可以达到最大响应速度。

3. 在 Color Depth（色彩深度）下拉列表上选择色彩深度。KX II-101 可以动态调整要给远程用户传输的色彩深度，使所有带宽的利用率最大。

15-bit RGB Color（15 位 RGB 色）

8-bit RGB Color（8 位 RGB 色）

4-bit Color（4 位色）

4-bit Gray（4 位灰度）

3-bit Gray（3 位灰度）

2-bit Gray（2 位灰度）

Black and White（黑白）

重要事项：对于大多数管理任务（服务器监视和重新配置等），不一定要使用大多数调制解调器显示卡支持的 24 位或 32 位全彩色。如果尝试传输这样高的色彩深度，只会浪费网络带宽。

---

4. 用滑块选择所需的 Smoothing（平滑）水平（仅 15 位彩色模式）。平滑水平决定了如何将色差较小的屏幕区变成平滑单色区。平滑功能可降低显示图像的噪声，从而提高目标服务器视频的效果。
5. 单击 OK（确定）按钮设置这些属性。

➢ *取消而不保存更改：*

- 单击 Cancel（取消）。

连接信息

➢ *获得有关 Virtual KVM Client 连接的信息：*

- 选择 Connection（连接）> Connection Info（连接信息）。打开 Connection Info（连接信息）窗口。

显示下列有关当前连接的信息：

- Device Name（设备名称）。KX II-101 设备的名称。
- IP Address（IP 地址）。KX II-101 设备的 IP 地址。
- Port（端口）。用于访问目标设备的 KVM 通信 TCP/IP 端口。
- Data In/Second（传入数据/秒）。传入的数据速率。
- Data Out/Second（传出数据/秒）。传出的数据速率。
- Connect Time（连接时间）。连接持续时间。
- FPS。每秒传输的视频帧。
- Horizontal Resolution（水平分辨率）。屏幕水平方向的分辨率。
- Vertical Resolution（垂直分辨率）。屏幕垂直方向的分辨率。
- Refresh Rate（刷新速率）。屏幕刷新速度。
- Protocol Version（协议版本）。RFB 协议版本。

➢ *复制这些信息：*

- 单击 Copy to Clipboard（复制到剪贴板）。可以把这些信息粘贴到您选择的程序里。

退出

➢ *关闭 Virtual KVM Client（当前访问的目标服务器）：*

- 选择 Connection（连接）> Exit（退出）。

键盘菜单

发送 Ctrl+Alt+Delete

由于 Ctrl+Alt+Delete 使用频繁，所以 Virtual KVM Client 预先编制了 Ctrl+Alt+Delete 宏。

此键序列被发送到当前连接的目标服务器。相反，如果您在使用 Virtual KVM Client 时按 Ctrl+Alt+Delete 键，由于操作系统结构的原因，该命令首先由您自己的 PC 截取，而不是按照预期的那样将该键序列发送到目标服务器。

	发送 Ctrl+Alt+Delete	将 Ctrl+Alt+Delete 键序列发送到目标服务器

➢ *将 Ctrl+Alt+Delete 键序列发送到目标服务器：*

- 选择 Keyboard（键盘）> Send Ctrl+Alt+Delete（发送 Ctrl+Alt+Delete），或者
- 单击工具栏上的 Send Ctrl+Alt+Delete（发送 Ctrl+Alt+Delete）按钮

键盘宏

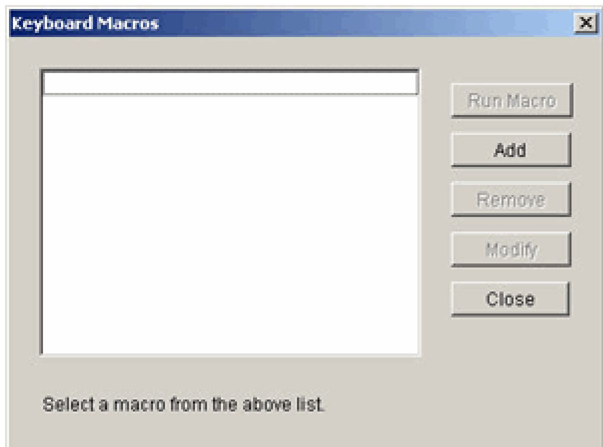
键盘宏可确保计划用于目标服务器的击键组合被发送到目标服务器，并且只由目标服务器截取。否则，这些击键组合可能会被运行 Virtual KVM Client 的计算机（您的客户机 PC）截获。

宏存储在客户机 PC 上，是 PC 专有的；因此，如果您使用另一台 PC，将看不到自己的宏。此外，如果另一个人使用您的 PC，并用不同的用户名登录，该用户将看到您的宏，因为宏是针对整个计算机的。在 Virtual KVM Client 上创建的键盘宏可在 MPC 上使用，反之亦然。

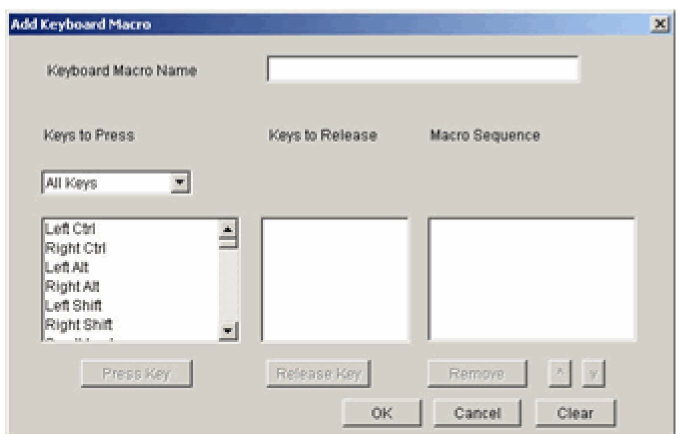
创建键盘宏

➢ *创建键盘宏（添加宏）：*

1. 选择 Keyboard（键盘）> Keyboard Macros（键盘宏）。打开 Keyboard Macro（键盘宏）对话框。



2. 单击 Add（添加）。打开 Add Keyboard Macro（添加键盘宏）对话框。



3. 在 Keyboard Macro Name（键盘宏名称）字段里输入名称。在创建宏之后，Virtual KVM Client 菜单栏将显示此名称。在此示例中，使用 Minimize All Windows（最小化所有窗口）。

4. 在 Keys to Press（要按的键）下拉列表上：

   a. 滚动并选择要模拟按键操作的每个键（按按键顺序）。

   b. 在每次选择之后，单击 Press Key（按键）。在选择每个键之后，Keys to Release（要释放的键）字段显示该键。

   在此示例中选择两个键：Windows 键和字母 D 键。

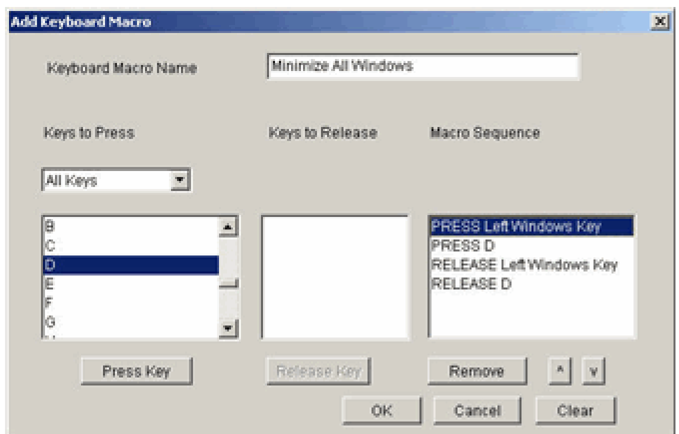
5. 在 Keys to Release（要释放的键）字段里：

   a. 选择要模拟其释放键操作的每个键（按释放顺序）。

   b. 在每次选择之后，单击 Release Key（释放键）。

   在此示例中，按下的两个键必须同时释放。

6. 检查 Macro Sequence（宏序列），该序列是用 Keys to Press（要按的键）和 Keys to Release（要释放的键）自动生成的。确定 Macro Sequence（宏序列）确实是您所希望的键序列。（如要删除序列中的一个步骤，选择该步骤，单击 Remove [删除]。）



提示：用 ^ 键和 v 键重新排序键序列。

7. 单击 Add Keyboard Macro（添加键盘宏）对话框上的 OK（确定）按钮保存宏。

8. 单击 Keyboard Macros（键盘宏）对话框上的 Close（关闭）。创建的键盘宏现在作为 Keyboard（键盘）菜单的菜单项列出：



➢ *清除所有字段并重新开始：*

- 单击 **Clear（清除）**按钮。

运行键盘宏

在创建键盘宏之后，可以在 Keyboard（键盘）菜单上单击宏名称执行它。

➢ *执行宏（使用本示例）：*

- 选择 Keyboard（键盘）> Minimize All Windows（最小化所有窗口）。

还有一种方法是在 Keyboard Macros（键盘宏）对话框上选择宏。

➢ *执行宏：*

1. 选择 Keyboard（键盘）> Keyboard Macros（键盘宏）。打开 Keyboard Macro（键盘宏）对话框。
2. 在列出的键盘宏中选择宏。
3. 单击 Run Macro（运行宏）。

修改键盘宏

➢ *修改宏：*

1. 选择 Keyboard（键盘）> Keyboard Macros（键盘宏）。打开 Keyboard Macro（键盘宏）对话框。
2. 在列出的键盘宏中选择宏。
3. 单击 Modify（修改）。打开 Add/Edit Macro（添加/编辑宏）对话框。
4. 修改宏。
5. 单击 OK（确定）。

删除键盘宏

➢ *删除宏：*

1. 选择 Keyboard（键盘）> Keyboard Macros（键盘宏）。打开 Keyboard Macro（键盘宏）对话框。
2. 在列出的键盘宏中选择宏。
3. 单击 Remove（删除）。宏被删除。

视频菜单

视频设置可以采用下列几种方式自动刷新：

- Refresh Screen（刷新屏幕）选项强制刷新视频屏幕
- Auto-sense Video Settings（自动检测视频设置）选项自动检测目标服务器的视频设置
- Calibrate Color（校准色彩）选项校准视频，改善显示色彩。

此外，可以用 Video Settings（视频设置）选项人工调整设置。

刷新屏幕

Refresh Screen（刷新屏幕）选项强制刷新屏幕。

	Refresh Screen（刷新屏幕）按钮

➢ *执行下列操作之一刷新视频设置：*

- 选择 Video（视频）> Refresh Screen（刷新屏幕）。
- 单击工具栏上的 Refresh Screen（刷新屏幕）按钮。

自动检测视频设置

Auto-sense Video Settings（自动检测视频设置）选项强制重新检测视频设置（分辨率和刷新速率），并刷新屏幕。

	Auto-Sense Video Settings（自动检测视频设置）按钮

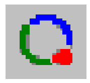
➢ *执行下列操作之一自动检测视频设置：*

- 选择 Video（视频）> Auto-sense Video Settings（自动检测视频设置）。
- 单击工具栏上的 Auto-sense Video Settings（自动检测视频设置）按钮。

显示一条消息，说明正在进行自动调整。

校准色彩

用 Calibrate Color（校准色彩）命令优化传输的视频图像的色彩级别（色调、亮度和饱和度）。KX II-101 色彩设置以目标服务器为基础。

	Calibrate Color（校准色彩）	调整色彩设置，优化视频显示。

注意：Calibrate Color（校准色彩）选项仅适用于当前连接。

➢ *校准色彩：*

1. 打开运行图形用户界面的任何目标服务器的远程 KVM 连接。
2. 选择 Video（视频）> Calibrate Color（校准色彩）（或者单击 Calibrate Color [校准色彩]按钮）。目标设备屏幕更新其色彩校准。

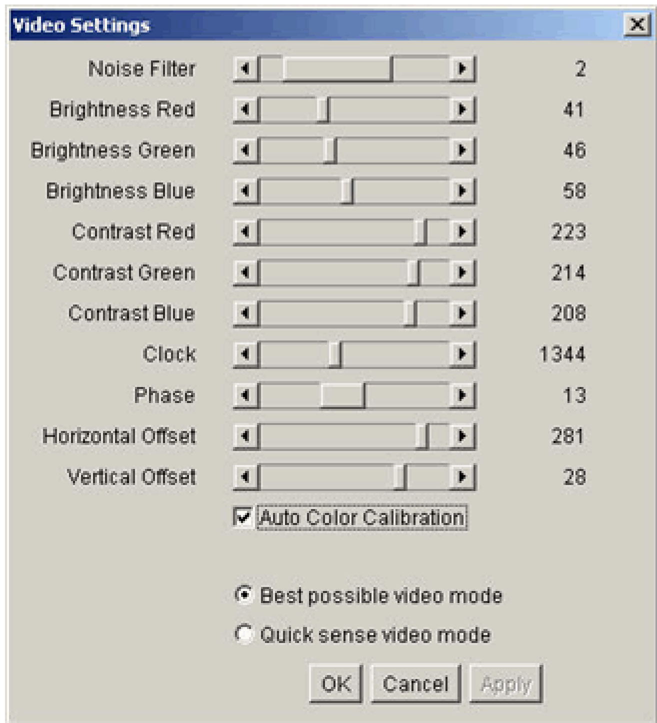
视频设置

用 Video Setting（视频设置）选项人工调整视频设置。

	Video Settings（视频设置）	打开 Video Settings（视频设置），人工调整视频参数。

➢ *更改视频设置：*

1. 选择 Video（视频）> Video Settings（视频设置）。打开 Video Settings（视频设置）对话框，显示当前设置：



2. 用滑块调整设置，实现所需的效果（在调整设置时，效果会立即显现出来）：

   - Noise Filter（噪声过滤器）。KX II-101 可以过滤显卡视频输出存在的电子干扰。此功能不仅优化图像质量，还降低所需的带宽。如果设置较高，只有在与相邻像素存在较大色差时，才传输不同的像素。但是，阈值设置过高会导致无意中过滤掉希望的屏幕变化。
     设置较低则要传输大部分像素变化。该阈值设置过低会增加带宽使用量。
   - Brightness（亮度）：此设置用于调整目标服务器的显示器亮度。
     - Red（红色）。控制红色信号的亮度。
     - Green（绿色）。控制绿色信号的亮度。
     - Blue（蓝色）。控制蓝色信号的亮度。
   - Color Contrast Settings（色彩对比度设置）：控制对比度调整。

- Contrast Red（红色对比度）。控制红色信号。
- Contrast Green（绿色对比度）。控制绿色信号。
- Contrast Blue（蓝色对比度）。控制蓝色信号。

- 如果视频图像看起来相当模糊或不聚焦，可以调整时钟和相位设置，直至活动目标服务器显示清晰图像为止。

警告：在更改时钟和相位设置时务必小心谨慎，因为这样做可能不显示图像或图像失真，可能无法返回之前的状态。在进行任何更改之前，与 Raritan 技术支持部门联系。

- Clock（时钟）。控制视频像素在屏幕上的显示速度。更改时钟设置会导致视频图像在水平方向上拉长或缩短，建议使用奇数设置。在大多数情况下，不应更改此设置，因为自动检测通常非常精确。
- Phase（相位）。相位值在 0-31 之间，是循环的。在活动目标服务器显示的图像达到最佳时，停止调整。

- Offset（偏移）：控制屏幕位置：
  - Horizontal Offset（水平偏移）。控制目标服务器在您的监视器上显示的水平位置。
  - Vertical Offset（垂直偏移）。控制目标服务器在您的监视器上显示的垂直位置。
- Auto Color Calibration（自动色彩校准）。如果要进行自动色彩校准，选择此选项。
- Video Sensing（视频检测）：选择视频检测模式：
  - Best possible video mode（最佳视频模式）：在切换目标服务器或目标分辨率时，KX II-101 执行完整的自动检测过程。选择此选项校准视频，实现最佳图像质量。
  - Quick sense video mode（快速检测视频）：使用此选项时，KX II-101 设备使用快速视频自动检测，尽快显示目标服务器视频。如果要在重新引导之后立即进入目标服务器的 BIOS 配置界面，此选项尤其有用。

3. 单击 Apply（应用）。Video Settings（视频设置）被更改了。

注意：某些 Sun 背景屏幕（例如有深黑色边框的屏幕）在某些 Sun 服务器上可能无法精确居中。使用不同的背景，或者在屏幕左上角放置一个颜色较浅的图标。

鼠标菜单

在控制远程服务器时，KX II-101 Remote Console 显示两个鼠标光标：一个是客户机工作站鼠标光标，另一个是目标服务器鼠标光标。您既可以在单鼠标模式下操作，也可以在双鼠标模式下操作。如果采用双鼠标模式且配置正确，这两个鼠标光标重叠在一起。如果鼠标同步有问题，参看配置目标服务器。

在两个鼠标光标不重叠时，KX II-101 提供下列几种鼠标模式：

- Absolute (Mouse Synchronization)（绝对[鼠标同步]）
- Intelligent (Mouse Mode)（智能[鼠标模式]）
- Standard (Mouse Mode)（标准[鼠标模式]）

同步鼠标

在双鼠标模式下，Synchronize Mouse（同步鼠标）强制目标服务器的鼠标指针与 Virtual KVM Client 的鼠标指针重叠在一起。

	Synchronize Mouse（同步鼠标）

➢ *执行下列操作之一同步鼠标：*

- 选择 Mouse（鼠标）> Synchronize Mouse（同步鼠标）。
- 单击工具栏上的 Synchronize Mouse（同步鼠标）按钮。

单鼠标光标

Single Mouse Cursor（单鼠标光标）进入单鼠标模式，只显示目标服务器鼠标光标，屏幕不再显示本地 PC 鼠标指针。在单鼠标模式下，Synchronize Mouse（同步鼠标）选项不可用（无需同步一个鼠标光标）。

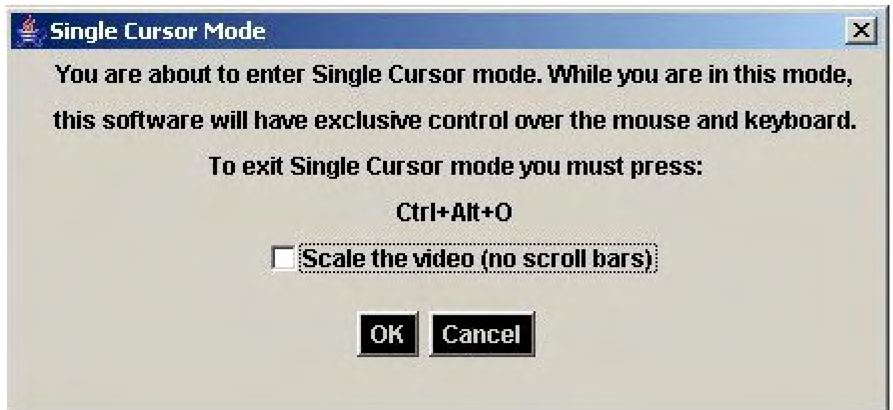
	Single Mouse Cursor（单鼠标光标）

➢ *执行下列操作之一进入单鼠标模式：*

- 选择 Mouse（鼠标）> Single Mouse Cursor（单鼠标光标）。
- 单击工具栏上的 Single/Double Mouse Cursor（单/双鼠标光标）按钮。

➢ *退出单鼠标模式：*

1. 在进入单鼠标模式之后，显示下列消息。单击 OK（确定）。



2. 按键盘上的 Ctrl+Alt+O 键退出单鼠标模式。

标准

这是采用相对鼠标位置的标准鼠标同步算法。标准鼠标模式要求禁用加速度，正确设置其他鼠标参数，这样客户机鼠标和服务器鼠标才能保持同步。标准鼠标模式是默认模式。

➢ *进入标准鼠标模式：*

- 选择 Mouse（鼠标）> Standard（标准）。

智能

在智能鼠标模式下，KX II-101 可以检测目标鼠标设置，据此同步鼠标指针，允许在目标服务器上启用鼠标加速度。在此模式下，鼠标光标在屏幕左上角跳动，并计算加速度。为了使此模式正常工作，必须满足某些条件。

如要进一步了解智能鼠标模式，参看 Raritan 网站 http://www.raritan.com/support/productdocumentation 上的《Raritan Multi-Platform Client 用户指南》（附录 B：智能鼠标同步条件），本指南也可以在随 KX II-101 一起提供的 Raritan User Manuals & Quick Setup Guides CD ROM 上找到。

➢ *进入智能鼠标模式：*

- 选择 Mouse（鼠标）> Intelligent（智能）。

智能鼠标同步条件

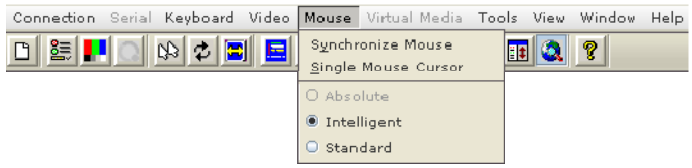
在鼠标闲置期间，Mouse（鼠标）菜单上的 Intelligent Mouse Synchronization（智能鼠标同步）命令自动同步鼠标光标。但为了使此功能正常工作，必须满足下列条件：

- 应该在目标服务器上禁用活动桌面。
- 目标页左上角不应显示任何窗口。
- 目标页左上角不应有动画背景。
- 目标鼠标光标的形状应当是普通形状，而不是动画形状。
- 目标鼠标的速度不应设置为太小或太大的值。
- 应该禁用 Enhanced pointer precision（提高指针精确度）或 Snap mouse to default button in dialogs（让光标对齐对话框上的默认按钮）等高级鼠标属性。
- 在 Video Settings（视频设置）窗口上选择 Best Possible Video Mode（最佳视频模式）。
- 目标视频的边缘应该很清晰，也就是说在滚动到目标视频图像边缘时，目标桌面和远程 KVM 控制台窗口之间的黑边框清晰可见。
- 在使用智能鼠标同步功能时，如果桌面左上角有文件图标或文件夹图标，可能会使该功能不能正常工作。为了避免此功能出问题，Raritan 建议您不要把文件图标或文件夹图标放在桌面左上角。

在自动检测目标视频之后，单击工具栏上的 Synchronize Mouse（同步鼠标）按钮，人工启动鼠标同步。如果在目标屏幕的分辨率发生变化时，不同的鼠标光标开始变得不同步，也可以使用智能鼠标同步。

如果智能鼠标同步失败，此模式将恢复标准鼠标同步特性。

请注意在不同的目标操作系统上，鼠标配置会有差异。参看操作系统指南了解详情。还要注意智能鼠标同步不适用于 UNIX 目标服务器。



绝对

注意：Absolute Mouse Synchronization（绝对鼠标同步）仅用于支持虚拟介质的 USB CIM (D2CIM-VUSB)。

在此模式下，用绝对坐标使客户机指针与目标服务器指针保持同步，即使目标服务器鼠标设置为不同的加速度或速度也如此。具备 USB 端口的服务器支持此模式；鼠标移动到目标服务器上的准确位置。

➢ *进入绝对鼠标模式：*

- 选择 Mouse（鼠标）> Absolute（绝对）。

虚拟介质

参看***虚拟介质*** (p. 94)一章，了解有关虚拟介质设置和使用的完整信息。

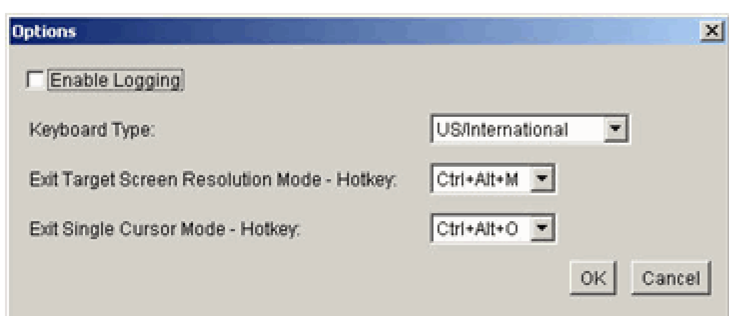
工具菜单

选项

可以在 Tools（工具）菜单上指定某些与 Virtual KVM Client 一起使用的选项：在双鼠标模式下同步鼠标、启用日志记录、键盘类型和退出目标屏幕分辨率模式热键。

➢ *设置工具选项：*

1. 选择 Tools（工具）> Options（选项）。打开 Options（选项）对话框。



2. 只有在得到技术支持部门的指示，才选择 Enable Logging（启用日志记录）复选框。此选项在主目录下创建一个日志文件。
3. 如果必要，在 Keyboard Type（键盘类型）下拉列表上选择键盘类型。这些选项包括：
   - US/International（美国英语/国际英语）
   - French (France)（法语[法国]）
   - German (Germany)（德语[德国]）
   - Japanese（日语）
   - United Kingdom（英国）
   - Korean (Korea)（朝鲜语[韩国]）
   - Belgian（比利时）
   - Norwegian（挪威语）
   - Danish（丹麦语）
   - Swedish（瑞典语）
4. Exit Target Screen Resolution Mode - Hotkey（退出目标屏幕分辨率模式 — 热键）。在进入目标屏幕分辨率模式时，目标服务器的显示器变成全屏，获得与目标服务器相同的分辨率。这是用于退出此模式的热键；在下拉列表上选择。
5. Exit Single Cursor Mode - Hotkey（退出单光标模式 — 热键）。在进入单光标模式时，只显示目标服务器鼠标光标。这是用于退出单光标模式的热键，重新显示客户机鼠标光标；在下拉列表上选择。
6. 单击 OK（确定）。

视图菜单

视图工具栏

可以在显示或不显示工具栏的情况下使用 Virtual KVM Client。

➢ *切换工具栏显示（打开和关闭）：*

- 选择 View（视图）> View Toolbar（视图工具栏）。

缩放

缩放目标窗口，可以看到目标服务器窗口的整个内容。此功能增大或缩小目标视频大小，使之适合 Virtual KVM Client 窗口大小，并保持长宽比不变，即使您不使用滚动条也能看到整个目标服务器桌面。

➢ *切换缩放（打开和关闭）：*

- 选择 View（视图）> Scaling（缩放）。

目标屏幕分辨率

在进入目标屏幕分辨率模式时，目标服务器的显示器变成全屏，获得与目标服务器相同的分辨率。在 Options（选项）对话框上指定用于退出此模式的热键（默认热键是 Ctrl+Alt+M）。

➢ *进入目标屏幕分辨率模式：*

- 选择 View（视图）> Target Screen Resolution（目标屏幕分辨率）。

➢ *退出目标屏幕分辨率模式：*

- 按在 Tools Options（工具选项）对话框上配置的热键。默认热键是 Ctrl+Alt+M。

CC-SG 用户须知：禁用 Target Screen Resolution（目标屏幕分辨率）；只有在 KX II-101 设备不受 CC-SG 管理时，才能使用全屏模式。

帮助菜单

关于 Raritan Virtual KVM Client

此菜单选项提供有关 Virtual KVM Client 的版本信息，这是在您需要 Raritan 技术支持部门的协助时应该了解的。

➢ *获取版本信息：*

- 选择 Help（帮助）> About Raritan Virtual KVM Client（关于 Raritan Virtual KVM Client）。

7 虚拟介质

在本章内

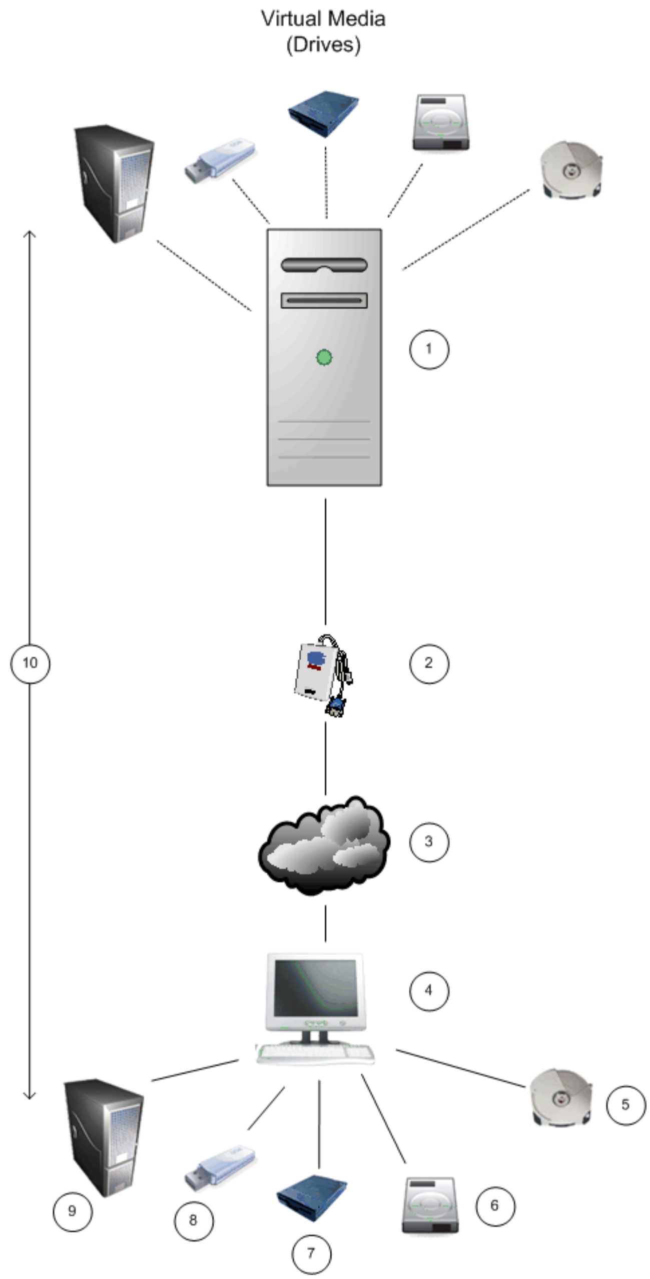
概述

虚拟介质允许 KVM 目标服务器远程访问客户机 PC 和网络文件服务器上的介质，从而扩展了 KVM 功能。在使用此功能时，安装在客户机 PC 和网络文件服务器上的介质基本上可由目标服务器虚拟加载。随后，目标服务器可以读写这些介质，就像读写与目标服务器直接相连的介质一样。虚拟介质包括内置和 USB 安装的 CD 驱动器和 DVD 驱动器、USB 大容量存储设备、PC 硬盘驱动器和软盘驱动器、ISO 映像（磁盘映像）。

虚拟介质使您能远程执行更多下面这样的任务：

- 传输文件
- 运行诊断
- 安装或修补应用程序
- 完成操作系统的安装（如果机器 BIOS 支持）

这种扩展 KVM 控制功能使您在大多数情况下不必亲自到数据中心去，可以节省时间和金钱。



1 目标服务器。

2 KX II-101

3 KX II-101 到本地工作站的 IP 网络连接。

4 本地工作站。

5 CD/ROM 驱动器。

6 硬盘驱动器映像文件。

7 软盘驱动器。

8 USB 驱动器。

9 远程文件服务器（ISO 映像）。

10 虚拟连接

使用虚拟介质的先决条件

为了使用虚拟介质，必须满足下列条件：

KX II-101

- 对于需要访问虚拟介质的用户，必须设置 KX II-101 权限，允许访问相关端口，还要设置这些端口对应的虚拟介质访问权（VM 访问端口权限）。端口权限在组级别设置；参看设备用户指南的设置端口权限部分了解详情。
- 在 KX II-101 和目标服务器之间必须有 USB 连接。
- 如果要使用 PC 共享，还必须在 Security Settings（安全设置）页上启用 VM 共享模式。**可选**
- 必须给要连接的 KVM 目标服务器选择正确的 USB 配置文件。如要了解如何选择 USB 配置文件，参看设备用户指南的设置 USB 配置文件部分。

客户机 PC

- 某些虚拟介质选项要求您有客户机 PC 管理权限（例如整个驱动器的驱动器重定向）。

> 注意：如果您使用 Microsoft Vista，要关闭 User Account Control（用户帐号控制）：Control Panel（控制面板）> User Accounts（用户帐号）> User Account Control（用户帐号控制）> turn off（关闭）。
>
> 如果不想更改 Vista 帐号权限，可以用管理员身份运行 Internet Explorer。为此，单击 Start（开始）菜单，找到 IE，用右键单击它，选择 Run as Administrator（作为管理员运行）。

- USB 2.0 端口速度更快，是首选端口。

目标服务器

- KVM 目标服务器必须支持 USB 连接的驱动器。
- 运行 Windows 2000 的 KVM 目标服务器必须安装了所有最新补丁。

使用虚拟介质

在使用 KX II-101 虚拟介质功能时，最多可以加载两个（不同类型的）驱动器。在整个 KVM 会话期间，均可访问这些驱动器。

➢ *使用虚拟介质：*

1. 将介质连接到您要在目标服务器上访问的客户机或网络文件服务器。此步骤不一定是第一步，但在尝试访问此介质之前必须这样做。
2. 确定是否满足适当的***先决条件*** (参看 "使用虚拟介质的先决条件" p. 97)。
3. （仅文件服务器 ISO 映像）如果要访问文件服务器 ISO 映像，通过 KX II-101 Remote Console ***文件服务器设置页*** (参看 "文件服务器设置（仅文件服务器 ISO 映像）" p. 103)确定这些文件服务器和映像。

   注意：ISO9660 格式是 Raritan 支持的标准格式。但是，也有可能使用其他 CD-ROM 扩展。

4. 用适当的目标服务器打开 KVM 会话。
5. 连接虚拟介质。

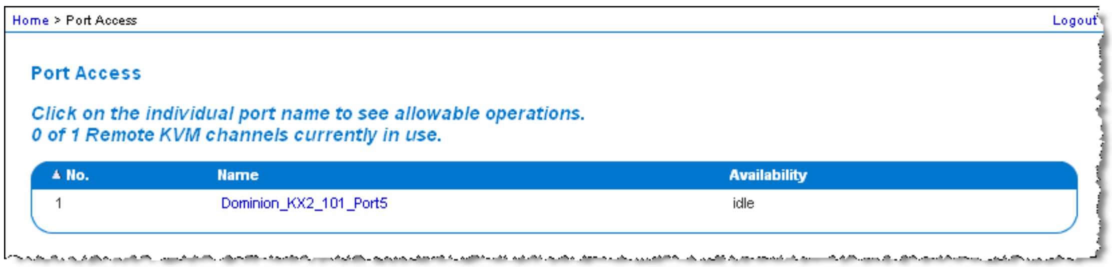
对于：	选择此 VM 选项：
本地驱动器	***Connect Drive（连接驱动器）*** (参看 "本地驱动器" p. 100)
本地 CD/DVD 驱动器	***Connect CD-ROM/ISO Image（连接 CD-ROM/ISO 映像）*** (参看 "CD-ROM/DVD-ROM/ISO 映像" p. 101)
ISO 映像	Connect CD-ROM/ISO Image（连接 CD-ROM/ISO 映像）
文件服务器 ISO 映像	Connect CD-ROM/ISO Image（连接 CD-ROM/ISO 映像）

在完成任务之后，***断开虚拟介质*** (p. 102)。

打开 KVM 会话

➢ *打开 KVM 会话：*

1. 在 KX II-101 Remote Console 上打开 Port Access（端口访问）页。



2. 在 Port Access（端口访问）页上连接目标服务器：

   a. 单击目标服务器的 Name（名称）。

   b. 在弹出菜单上选择 Connect（连接）。



在 Virtual KVM Client 窗口上打开目标服务器。

连接虚拟介质

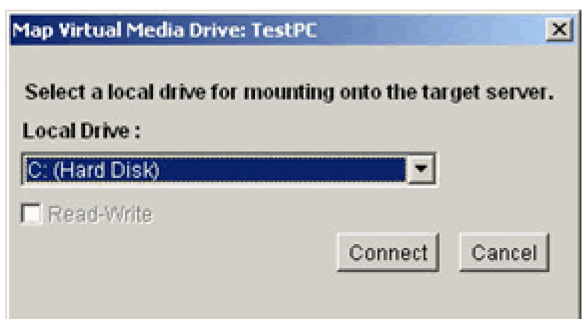
本地驱动器

此选项加载一个驱动器；磁盘驱动器被虚拟加载到目标服务器上。此选项只用于硬盘驱动器和外置驱动器，不包括网络驱动器、CD-ROM 驱动器或 DVD-ROM 驱动器。这是唯一一个可供读写的选项。

注意：在 NTFS 格式化分区（如本地 C 盘驱动器）重定向到新的大容量存储连接之后，运行某些 Windows 操作系统版本的目标服务器可能不能接受这些连接。如果发生这种情况，关闭 KX II-101 Remote Console 再重新连接，然后重定向另一个虚拟介质设备。如果其他用户连接同一台目标服务器，他们也必须关闭目标服务器连接。

➢ *访问客户机计算机上的驱动器：*

1. 在 Virtual KVM Client 上选择 Virtual Media（虚拟介质）> Connect Drive（连接驱动器）。打开 Map Virtual Media Drive（映射虚拟介质驱动器）对话框。



2. 在 Local Drive（本地驱动器）下拉列表上选择驱动器。

3. 如果需要读写功能，选择 Read-Write（读写）复选框。对于固定驱动器，此选项被禁用。参***看在什么情况下读写不可用*** (参看 "在什么情况下读写不可用" p. 101)部分了解详情。在选择此选项之后，可以读写所连接的 USB 磁盘。

   警告：启用读写访问可能很危险！多个实体同时访问同一个驱动器可能会造成数据损坏。如果不需要写访问，不要选择此选项。

4. 单击 Connect（连接）。介质将被虚拟加载到目标服务器上。您可以像访问其他任何驱动器一样访问该介质。

   注意：如果没有至目标服务器的 USB 连接，将显示一条警告消息："设置了虚拟介质功能，但在连接 USB 电缆或接通目标服务器电源之前不可用。请检查 USB 连接，或者检查目标服务器是否通电了。"先解决此问题，再连接驱动器。

在什么情况下读写不可用

在下列情况下，不能使用虚拟介质读/写功能：

- 对于所有硬盘驱动器。
- 当驱动器有写保护时。
- 当用户没有读/写权限时：
  - Port Permission Access（端口权限访问）被设置为 None（无）或 View（查看）
  - Port Permission VM Access（端口权限 VM 访问）被设置为 Read-Only（只读）或 Deny（拒绝）

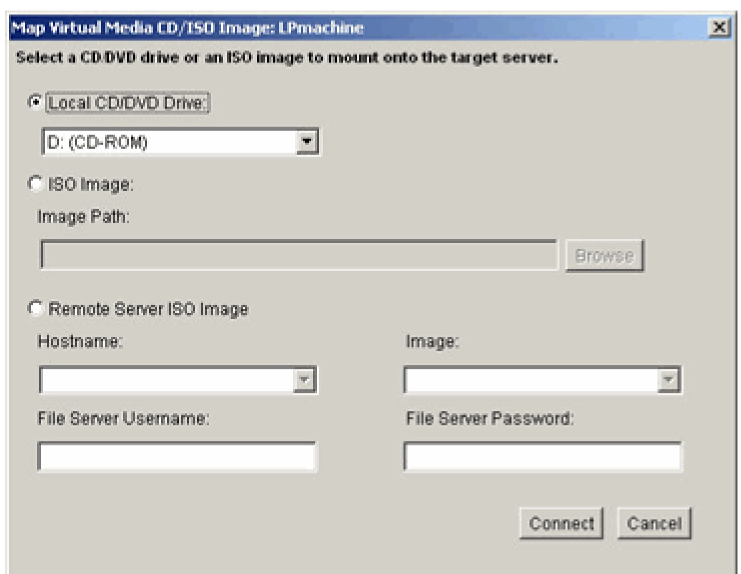
CD-ROM/DVD-ROM/ISO 映像

此选项加载 CD-ROM、DVD-ROM 和 ISO 映像。

注意：ISO9660 格式是 Raritan 支持的标准格式。但是，也有可能使用其他 CD-ROM 扩展。

➢ *访问 CD-ROM、DVD-ROM 或 ISO 映像：*

1. 在 Virtual KVM Client 上选择 Virtual Media（虚拟介质）> Connect CD-ROM/ISO Image（连接 CD-ROM/ISO 映像）。打开 Map Virtual Media CD/ISO Image（映射虚拟介质 CD/ISO 映像）对话框。



2. 对于内置和外置 CD-ROM 驱动器或 DVD-ROM 驱动器：
   a. 选择 Local CD/DVD Drive（本地 CD/DVD 驱动器）选项。

b. 在 Local CD/DVD Drive（本地 CD/DVD 驱动器）下拉列表上选择驱动器。所有可用的内置和外置 CD 驱动器和 DVD 驱动器的名称将出现在下拉列表上。

c. 单击 Connect（连接）。

3. 对于 ISO 映像：

a. 选择 ISO Image（ISO 映像）选项。如果要访问 CD 驱动器、DVD 驱动器或硬盘驱动器的磁盘映像，使用此选项。ISO 格式是唯一支持的格式。

b. 单击 Browse（浏览）按钮。

c. 找到您要使用的磁盘映像所在的路径，单击 Open(打开)。Image Path（映像路径）字段显示该路径。

d. 单击 Connect（连接）。

4. 对于文件服务器上的远程 ISO 映像：

a. 选择 Remote Server ISO Image（远程服务器 ISO 映像）选项。

b. 在 Hostname（主机名）下拉列表和 Image（映像）下拉列表上选择主机名和映像。可用的文件服务器和映像路径是您用 File Server Setup（文件服务器设置）页配置的服务器和路径。下拉列表只显示您用 KX II-101 File Server Setup（文件服务器设置）页配置的项目。

c. File Server Username（文件服务器用户名）。访问文件服务器所需的用户名。

d. File Server Password（文件服务器密码）。访问文件服务器所需的密码（当您输入时，该字段将屏蔽）。

e. 单击 Connect（连接）。

介质将被虚拟加载到目标服务器上。您可以像访问其他任何驱动器一样访问该介质。

断开虚拟介质

➢ *断开虚拟介质驱动器：*

- 对于本地驱动器，选择 Virtual Media（虚拟介质）> Disconnect Drive（断开驱动器）。
- 对于 CD-ROM、DVD-ROM 和 ISO 映像，选择 Virtual Media（虚拟介质）> Disconnect CD-ROM/ISO Image（断开 CD-ROM/ISO 映像）。

注意：除了用 Disconnect（断开）选项断开虚拟介质，也可以在关闭 KVM 连接时关闭虚拟介质。

文件服务器设置（仅文件服务器 ISO 映像）

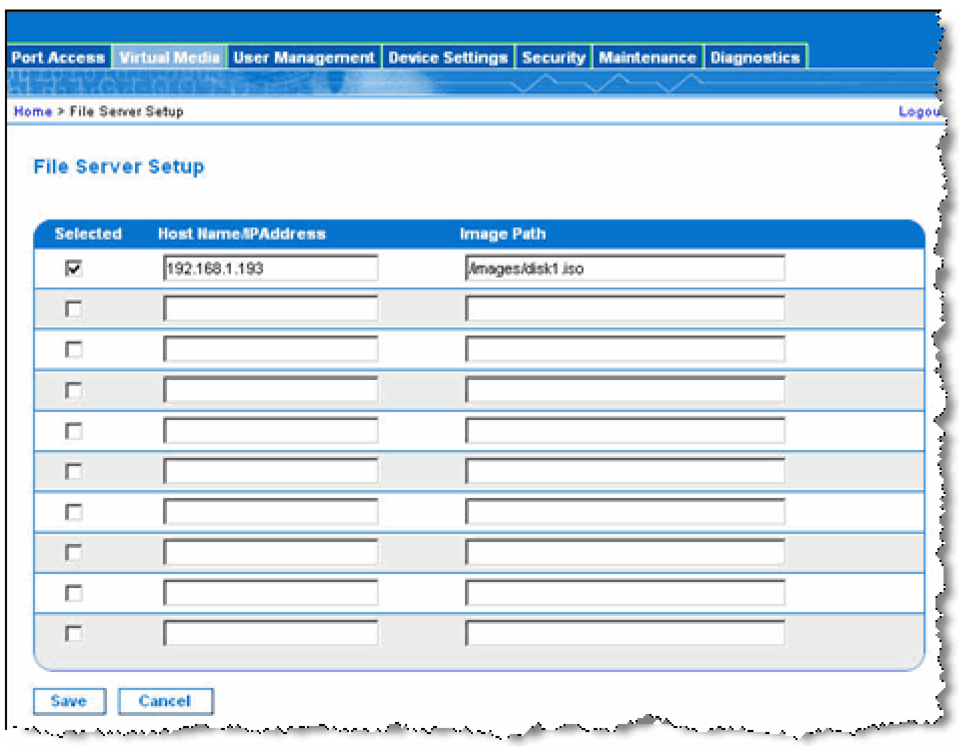
注意：仅当用虚拟介质访问文件服务器 ISO 映像时，才需要此功能。

注意：ISO9660 格式是 Raritan 支持的标准格式。但是，可能也能使用其他 CD-ROM 扩展。

用 KX II-101 Remote Console 的 File Server Setup（文件服务器设置）页指定要用 KX II-101 虚拟介质访问的文件服务器和映像路径。在此指定的文件服务器 ISO 映像，可以在（***Map Virtual Media CD/ISO Image dialog [映射虚拟介质 CD/ISO 映像对话框]*** (参看 "CD-ROM/DVD-ROM/ISO 映像" p. 101) 上的）Remote Server ISO Image Hostname（远程服务器 ISO 映像主机名）和 Image（映像）下拉列表上选择。

➢ *指定用于虚拟介质访问的文件服务器 ISO 映像：*

1. 在 KX II-101 Remote Console 上选择 Virtual Media（虚拟介质）。打开 File Server Setup（文件服务器设置）页。



2. 输入有关要访问的文件服务器 ISO 映像的信息：
   - Host Name/IP Address（主机名/IP 地址）。文件服务器的主机名或 IP 地址。
   - Image Path（映像路径）。ISO 映像位置的全路径名。

3. 选择要作为虚拟介质访问的所有介质对应的 Selected（选择）复选框。
4. 单击 Save（保存）。在此指定的所有介质，可以在 Map Virtual Media CD/ISO Image（映射虚拟介质 CD/ISO 映像）对话框上选择。

8 设备管理

在本章内

设备设置菜单

Device Settings（设备设置）菜单有下列菜单项：Network（网络）、Device Services（设备服务）、Keyboard/Mouse（键盘/鼠标）、Serial Port（串行端口）、Date/Time（日期/时间）、Event Management - Settings（事件管理 — 设置）、Event Management - Destinations（事件管理 — 目标）和 Port Configuration（端口配置）。

使用：	目的：
Network（网络）	定制 KX II-101 网络配置。
Device Services（设备服务）	配置 KX II-101 网络端口，启用 TELNET 和 SSH 访问。
Keyboard/Mouse（键盘/鼠标）	配置目标服务器如何看到 KX II-101 发送的键盘信号和鼠标信号。
Serial Port（串行端口）	选择和配置 KX II-101 串行端口的功能。
Date/Time（日期/时间）	设置日期、时间、时区和网络时间协议 (NTP)。
Event Management - Settings（事件管理 — 设置）	配置 SNMP 和 Syslog。
Event Management - Destinations（事件管理 – 目标）	选择要跟踪哪些系统事件，以及要把这些信息发送到哪里。
Port Configuration（端口配置）	配置 KVM 端口和插座。

Network Settings（网络设置）

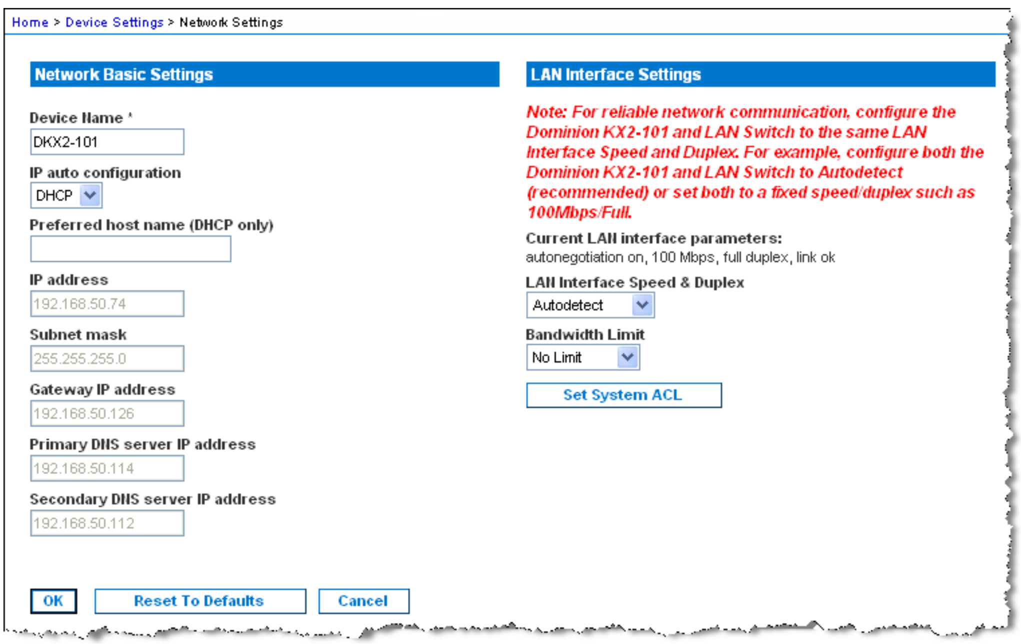
用 Network Settings（网络设置）页定制 KX II-101 设备的网络配置（例如 IP 地址、发现端口和 LAN 接口参数）。

设置 IP Configuration（IP 配置）主要有两种方法：

- None（无）。（默认值）此选项是建议的选项（静态 IP）。由于 KX II-101 是网络基础结构的一部分，您很可能不希望其 IP 地址频繁变化。可以用此选项设置网络参数。
- DHCP。IP 地址由 DHCP 服务器自动分配。

➢ *更改网络配置：*

1. 选择 Device Settings（设备设置）> Network（网络）。打开 Network Settings（网络设置）页。



2. 更新 Network Basic Settings（网络基本设置）。参看网络基本设置部分了解每个字段。
3. 更新 LAN Interface Settings（LAN 接口设置）。参看 LAN 接口设置部分了解每个字段。
4. 单击 OK（确定）按钮设置这些配置。如果所做的更改要求重新引导设备，将显示一条重新引导消息。

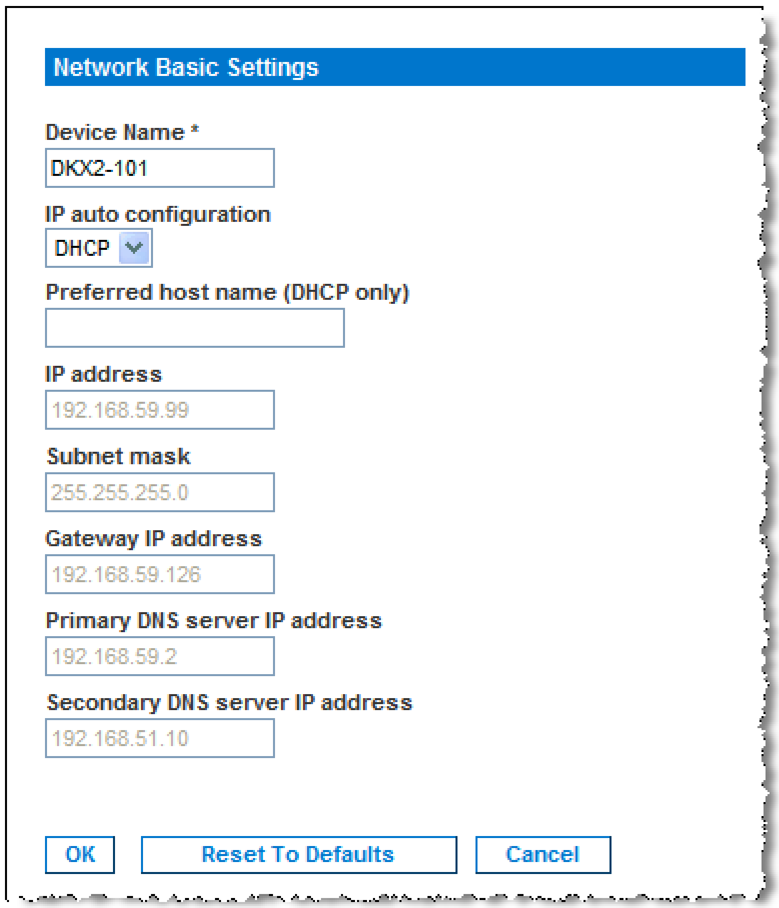
➢ *取消而不保存更改：*

- 单击 Cancel（取消）。

➢ *恢复到出厂默认值：*

- 单击 Reset to Defaults（恢复默认值）。

网络基本设置



- Device Name（设备名称）。输入唯一设备名称（最长 16 个字符，不允许使用空格）。命名设备，使其很容易识别。KX II-101 设备的默认名称是：DKX2-101。远程用户也将看到此名称。但是，如果 MPC 用户给此设备创建了 Connection Profile（连接配置文件），该用户将看到连接配置文件中的 Description（说明）字段。
- IP auto configuration（IP 自动配置）。在下拉列表上的可用选项中选择：
  - None（无）。如果不需要自动 IP 配置，更愿意自己设置 IP 地址（静态 IP），使用此选项。此选项是建议的默认选项。

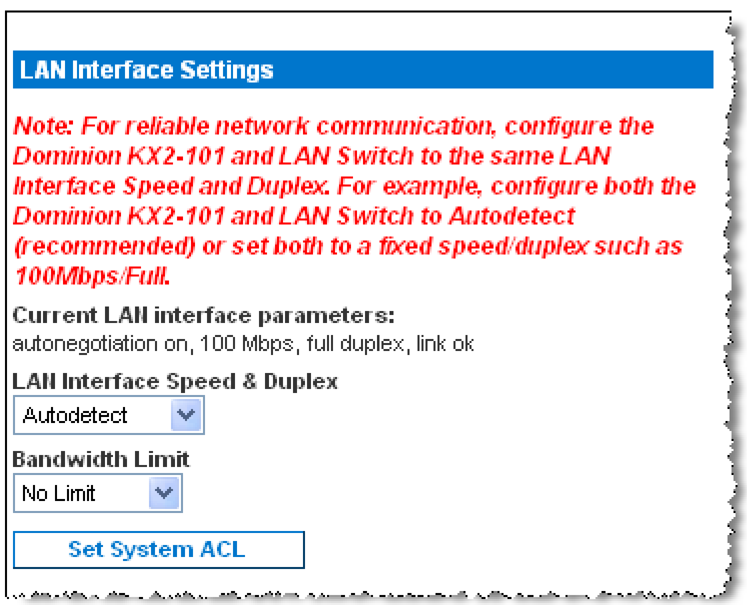
如果选择此选项进行 IP 自动配置，将启用下列 Network Basic Settings（网络基本设置）字段，您可以人工设置 IP 配置。

- IP Address（IP 地址）。默认 IP 地址是 192.168.0.192。
- Subnet Mask（子网掩码）。默认子网掩码是 255.255.255.0。
- Gateway IP Address（网关 IP 地址）。网关的 IP 地址（如果使用）。
- Primary DNS Server IP Address（主 DNS 服务器 IP 地址）。用于将名称转换成 IP 地址的主域名服务器。
- Secondary DNS Server IP Address（备用 DNS 服务器 IP 地址）。用于将名称转换成 IP 地址的备用域名服务器（如果使用）。

- DHCP。联网计算机（客户机）使用 Dynamic Host Configuration Protocol（动态主机配置协议），获取 DHCP 服务器分配的唯一 IP 地址和其他参数。

如果使用 DHCP，输入 Preferred host name（首选主机名）（仅限于 DHCP）。最长 63 个字符。

LAN 接口设置



- Current LAN interface parameters（当前 LAN 接口参数）字段显示当前参数设置。
- LAN Interface Speed & Duplex（LAN 接口速度和双工）。在可用的速度和双工组合中选择。

Autodetect（自动检测）	默认选项	
100 Mbps/Half（10 Mbps/半）		两个 LED 闪烁
1000 Mbps/Full（10 Mbps/全）		两个 LED 闪烁
100 Mbps/Half（100 Mbps/半）		黄色 LED 闪烁
100 Mbps/Full（100 Mbps/全）		黄色 LED 闪烁
1000 Mbps/Full（1000 Mbps/全）	千兆	绿色 LED 闪烁

半双工提供双向通信，但每次只允许一个方向通信（不允许两个方向同时通信）。

全双工允许同时进行双向通信。

注意：在半双工或全双工通信中，以 10 Mbps 运行时偶尔会出问题。如果出问题，尝试使用另一个速度和双工。

参看网络速度设置部分了解详情。

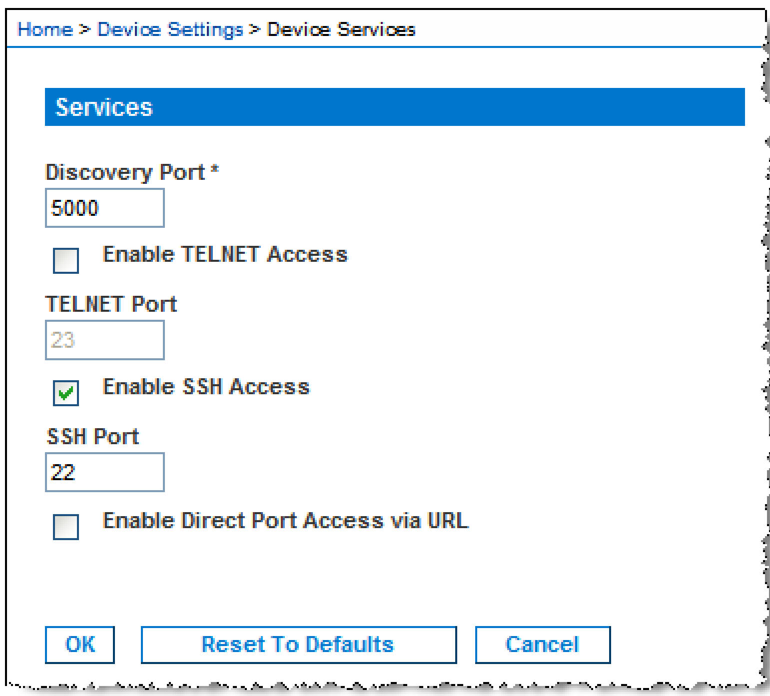
- Bandwidth Limit（带宽极限）。在可用的带宽选项中选择：
  - 128 Kb
  - 256 Kb
  - 512 Kb
  - 2 Mb
  - 5 Mb
  - 10 Mb
  - 100 Mb
  - 不限制

- Set System ACL（设置系统 ACL）。单击此按钮给 KX II-101 设置全局访问控制表，确保设备不响应来自被禁 IP 地址的数据包。打开 ***IP 访问控制*** (p. 139) 页。

注意：这些 ACL 值是全局性的，影响整个 KX II-101 设备。您也可以根据组创建 ACL。例如可以创建一个 Outsourced Vendors（外包供应商）用户组，只允许其 IP 地址在给定 IP 地址范围内的用户访问 KX II-101（参看基于组的 IP ACL 部分，了解如何创建组特定的访问控制表）。

设备服务

用 Device Services（设备服务）页指定 KX II-101 的连接选项。



➢ *配置发现端口：*

1. 选择 Device Settings（设备设置）> Device Services（设备服务）。打开 Device Services（设备服务）页。
2. 输入 KX II-101 与客户机 PC 通信所用的网络端口。
3. 单击 Save（保存）按钮保存设置。

➢ *启用 TELNET 访问：*

1. 选择 Device Settings（设备设置）> Device Services（设备服务）。打开 Device Services（设备服务）页。
2. 选择 Enable TELNET Access（启用 TELNET 访问）：

3. 输入对 KX II-101 进行 TELNET 访问所用的网络端口。
4. 单击 Save（保存）按钮保存设置。

➢ *启用 SSH 访问：*

1. 选择 Device Settings（设备设置）> Device Services（设备服务）。打开 Device Services（设备服务）页。
2. 选择 Enable SSH Access（启用 SSH 访问）：
3. 输入对 KX II-101 进行 SSH 访问所用的网络端口。
4. 单击 Save（保存）按钮保存设置。

启用直接端口访问

直接端口访问允许您直接访问 KX II-101 Remote Client，无需使用常用的登录页。在启用直接端口访问之后，您可以定义一个 URL，直接导航到 Port Access（端口访问）页。

➢ *启用直接端口访问：*

1. 选择 Device Settings（设备设置）> Device Services（设备服务）。打开 Device Services（设备服务）页。
2. 选择 Enable Direct Port Access via URL（通过 URL 启用端口访问）复选框。
3. 单击 Save（保存）按钮保存设置。

➢ *定义直接端口访问 URL：*

- 用 KX II-101 的 IP 地址、用户名、密码和端口号（必要时）定义一个 URL。如果只有一个 KVM 端口，不需要端口号。

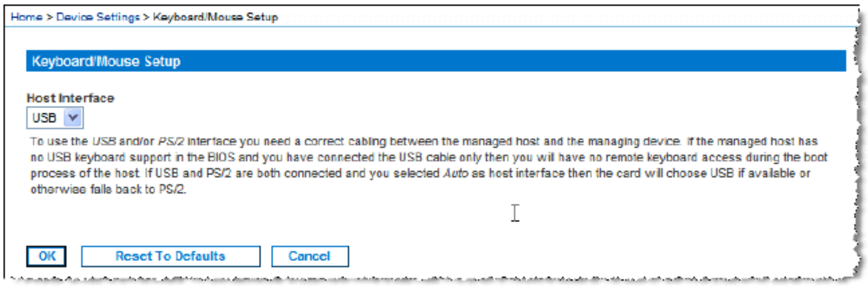
  直接端口访问 URL 的格式如下：

  https://[**IP address**]/dpa.asp?username=[**username**]&password=[**password**]&port=[**port number**]

提示：一旦定义直接端口访问 URL，就在浏览器里把它保存成书签，便于重复使用。

键盘/鼠标设置

用 Keyboard/Mouse Setup（键盘/鼠标设置）页配置 KX II-101 和主机设备之间的键盘接口和鼠标接口。



- Host Interface（主机接口）。选择 KX II-101 是通过 PS/2 连接还是 USB 连接发送键盘数据和鼠标数据。
  - Auto（自动）。在选择此设置之后，如果 USB 连接可用，KX II-101 将使用此连接，否则使用 PS/2 连接。
  - USB。强制 KX II-101 用 USB 连接将键盘数据和鼠标数据发送到主机设备。
  - PS/2。强制 KX II-101 用 PS/2 连接将键盘数据和鼠标数据发送到主机设备。

➢ *恢复出厂默认值*

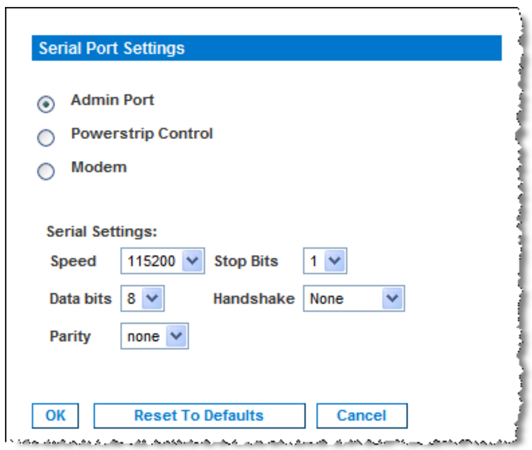
- 单击 Reset to Defaults（恢复默认值）。

串行端口设置

用 Serial Port Settings（串行端口设置）页设置 KX II-101 如何使用集成的串行端口。

➤ *配置串行端口：*

1. 选择 Device Settings（设备设置）> Serial Port（串行端口打开 Serial Port Settings（串行端口设置）页。



2. 给串行端口选择要使用的功能：
   - Admin Port（管理端口）。为了访问高级配置，选择此选项直接用客户机 PC 连接 KX II-101。
   - PowerStrip Control（电源板控制）。如果将 KX II-101 连接到串行控制的电源板，选择此选项。
   - Modem（调制解调器）。如果要将外置调制解调器连接到 KX II-101 提供拨号访问，选择此选项。
3. 对于 Modem（调制解调器）选项，如下配置调制解调器使用设置：
   a. 在 Serial line speed（串行线路速度）下拉列表上选择 KX II-101 和调制解调器之间的数据速度。
   b. 输入 Modem init 字符串。
   c. 输入 Modem server IP address（调制解调器服务器 IP 地址）。这是在用户通过调制解调器建立连接之后输入的用于访问 KX II-101 web 界面的地址。
   d. 输入 Modem client IP address（调制解调器客户机 IP 地址）。这是在用户通过调制解调器建立连接之后，给他/她分配的地址。
4. 单击 OK（确定）。

日期/时间设置

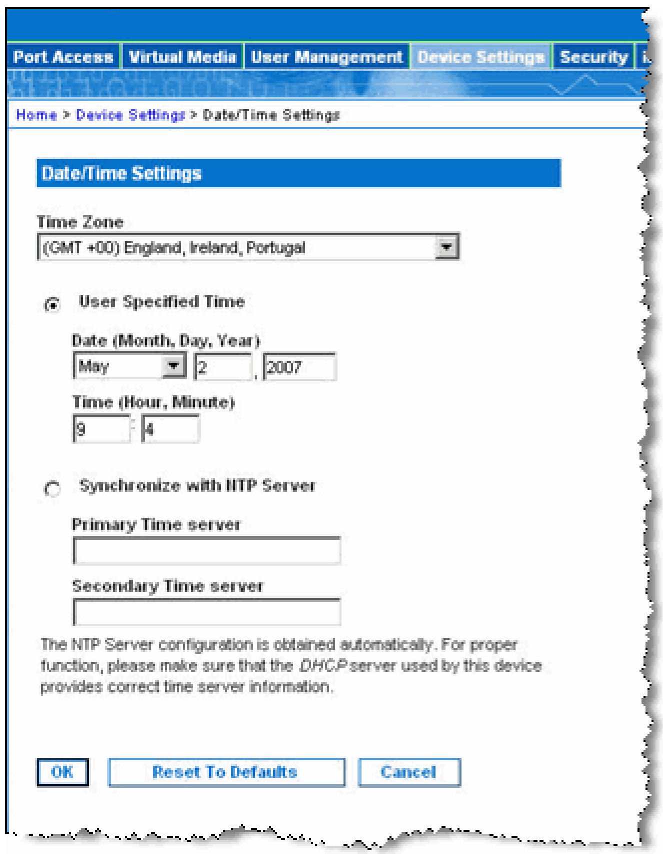
用 Date/Time Settings（日期/时间设置）页给 KX II-101 指定的日期和时间。有两种指定方法：

- 人工设置日期和时间，或者
- 与网络时间协议 (NTP) 服务器同步。

注意：KX II-101 不支持夏令时。

➢ *设置日期和时间：*

1. 选择 Device Settings（设备设置）> Date/Time（日期/时间）。打开 Date/Time Settings（日期/时间设置）页。



2. 在 Time Zone（时区）下拉列表上选择时区。
3. 选择要用于设置日期和时间的方法：
   - User Specified Time（用户指定的时间）。选择此选项，人工输入日期和时间。

- Synchronize with NTP Server（与 NTP 服务器同步）。选择此选项，使日期和时间与网络时间协议 (NTP) 服务器同步。

4. 对于 User Specified Time（用户指定的时间）选项，如下输入日期和时间：
   a. 在 Month（月份）下拉列表上选择月份。
   b. 输入 Day（日期）。
   c. 按 yyyy 格式输入 Year（年份）。
   d. 按 hh:mm 格式输入 Time（时间）（采用 24 小时制）。
5. 对于 Synchronize with NTP Server（与 NTP 服务器同步）选项：
   a. 输入 Primary Time server（主时间服务器）的 IP 地址。
   b. （可选）输入 Secondary Time server（备用时间服务器）的 IP 地址。
6. 单击 OK（确定）。

事件管理

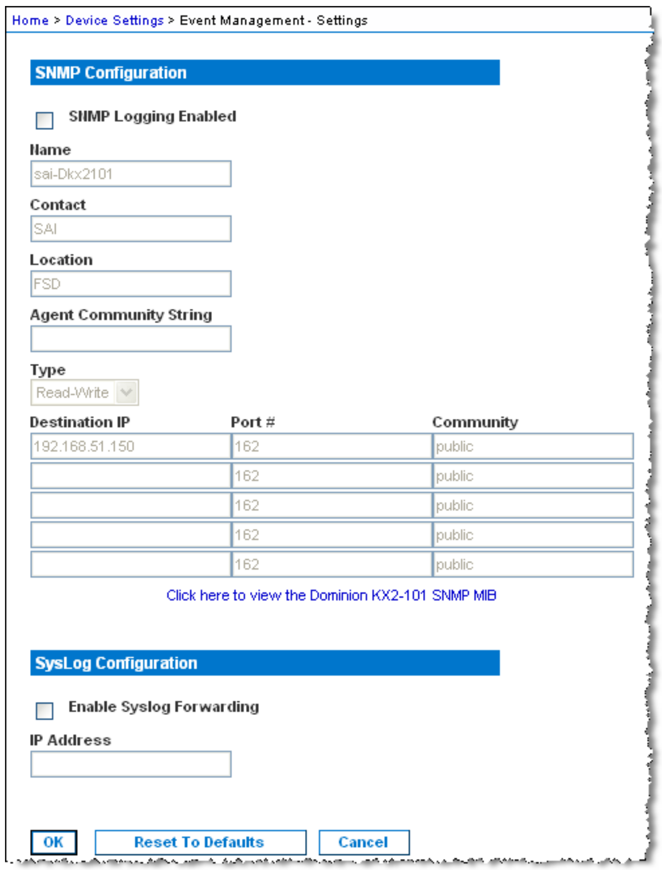
KX II-101 事件管理功能提供一组屏幕，用于允许和禁止向 SNMP 管理器、Syslog 和审计日志分发系统事件。这些事件都进行了分类，您可以针对每个事件确定是否要将它发送到一个或多个目标。

SNMP 配置

Simple Network Management Protocol (SNMP) 是用于控制网络管理和监视网络设备及其功能的协议。KX II-101 通过 Event Management（事件管理）提供 SNMP 代理支持。参看 ***SNMP 代理配置*** (p. 119)和 ***SNMP 陷阱配置*** (p. 119)，了解 SNMP 代理和陷阱。

➤ *配置 SNMP（启用 SNMP 记录）：*

1. 选择 Device Settings（设备设置）> Event Management – Settings（事件管理 — 设置）。打开 Event Management – Settings（事件管理 — 设置）页：

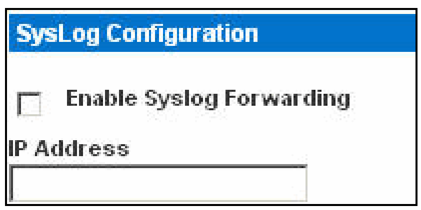


2. 选择 Enable SNMP Logging（启用 SNMP 记录）选项，启用其余 SNMP 字段。

3. 在 Name（姓名）、Contact（联系人）和 Location（位置）字段里分别输入 SNMP 代理的（此 Dominion 设备的）名称（如 KX II-101 控制台界面所显示的），与此设备有关的联系人姓名，以及此 Dominion 设备的物理位置。

4. 输入 Agent Community String（代理社区字符串）（Dominion 设备的字符串）。SNMP 社区是运行 SNMP 的设备和管理站所属的组，它有助于定义要把信息发送到哪里。社区名用于标识该组；一个 SNMP 设备或代理可能属于多个 SNMP 社区。
5. 用 Type（类型）下拉列表指定社区是 Read-Only（只读）还是 Read-Write（读写）。
6. 指定 SNMP 管理器的 Destination IP（目标 IP）、Port #（端口号）和 Community（社区），最多可以配置 5 个 SNMP 管理器。
7. 单击 Click here to view the KX II-101 SNMP MIB（单击这里查看 KX II-101 SNMP MIB）链接，访问 SNMP Management Information Base（SNMP 管理信息库）。
8. 单击 OK（确定）。

Syslog 配置



➢ *配置 Syslog（启用 Syslog 转发）：*

1. 选择 Enable Syslog Forwarding（启用 Syslog 转发）选项，将设备消息记录到远程 Syslog 服务器上。
2. 在 IP Address（IP 地址）字段里输入 Syslog 服务器的 IP 地址。
3. 单击 OK（确定）。

➢ *取消而不保存更改：*

- 单击 Cancel（取消）。

➢ *恢复到出厂默认值：*

- 单击 Reset to Defaults（恢复默认值）按钮。

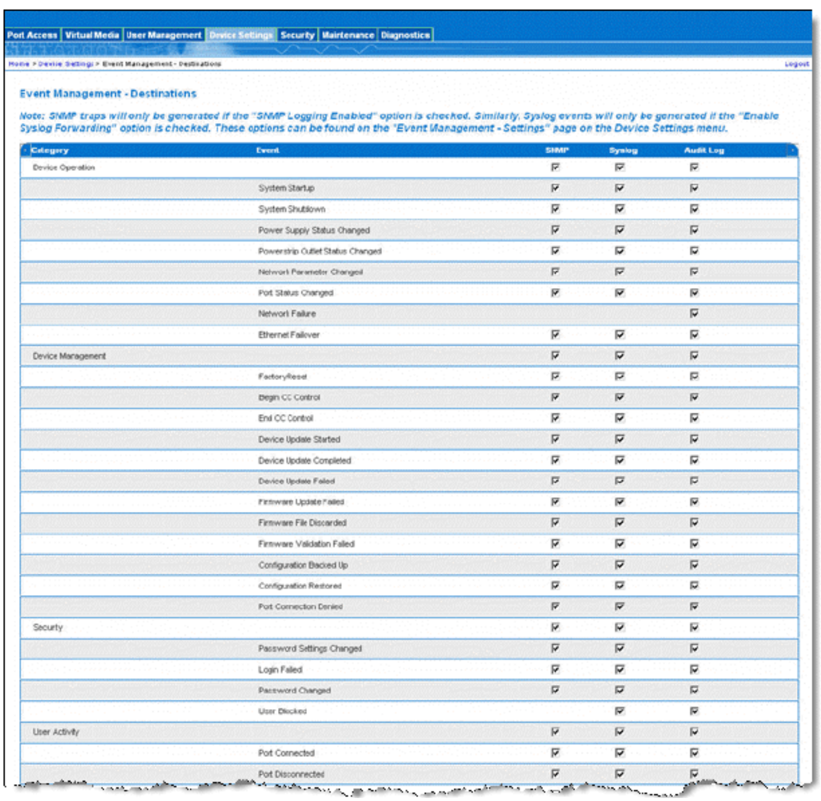
事件管理 — 目标

在启用系统事件之后，系统事件可以生成 SNMP 通知事件（陷阱），还可以记录到 Syslog 或审计日志里。用 Event Management - Destinations（事件管理 — 目标）页选择要跟踪哪些系统事件，以及要把这些信息发送到哪里。

注意：仅当选择 SNMP Logging Enabled（启用 SNMP 记录）选项时，才生成 SNMP 陷阱；仅当选择 Enable Syslog Forwarding（启用 Syslog 转发）选项时，才生成 Syslog 事件。这两个选项都在 Event Management - Settings（事件管理 — 设置）页上。参看事件管理 — 设置。

➢ *选择事件及其目标：*

1. 选择 Device Settings（设备设置）> Event Management – Destinations（事件管理 — 目标）。打开 Event Management – Destinations（事件管理 — 目标）页：



系统事件按 Device Operation（设备操作）、Device Management（设备管理）、Security（安全）、User Activity（用户活动）和 User Group Administration（用户组管理）进行分类。

2. 选择要启用或禁用的那些 Event（事件）项目对应的复选框，以及要把这些信息发送到哪里。

提示：分别选择或清除 Category（类别）项目复选框，启用或禁用整个 Category（类别）。

3. 单击 OK（确定）。

➢ *取消而不保存更改：*

- 单击 Cancel（取消）。

➢ *恢复到出厂默认值：*

- 单击 Reset to Defaults（恢复默认值）按钮。

警告：在使用基于 UDP 的 SNMP 陷阱时，如果重新引导 KX II-101，KX II-101 和它相连的路由器可能不同步，以致不能记录 SNMP 陷阱 "reboot completed"。

SNMP 代理配置

符合 SNMP 规范的设备（称为代理）将有关它们的数据存储在管理信息库 (MIB) 里，并将这些数据返回给 SNMP 管理器。用 Event Logging（事件记录）页配置 KX II-101（SNMP 代理）和 SNMP 管理器之间的 SNMP 连接。

SNMP 陷阱配置

在符合一个或多个条件时，SNMP 可以发送陷阱或通知，告知管理员。下表列出 KX II-101 SNMP 陷阱：

陷阱名称	说明
configBackup	设备配置已备份。
configRestore	设备配置已恢复。
deviceUpdateFailed	设备更新失败。
deviceUpgradeCompleted	KX II-101 通过 RFP 文件完成更新。
deviceUpgradeStarted	KX II-101 通过 RFP 文件开始更新。
factoryReset	设备已恢复到出厂默认值。
firmwareFileDiscarded	固件文件已被丢弃。
firmwareUpdateFailed	固件更新失败。
firmwareValidationFailed	固件确认失败。
groupAdded	组已被添加到 KX II-101 系统。
groupDeleted	组已从系统中删除。

陷阱名称	说明
groupModified	组已修改。
ipConflictDetected	检测到 IP 地址冲突。
ipConflictResolved	IP 地址冲突已解决。
networkFailure	该产品的 Ethernet 接口不能再进行网络通信。
networkParameterChanged	更改了网络参数。
passwordSettingsChanged	强密码设置已更改。
portConnect	此前验证的用户已开始 KVM 会话。
portConnectionDenied	到目标端口的连接被拒绝了。
portDisconnect	参与 KVM 会话的用户正确关闭了会话。
portStatusChange	端口不再可用。
powerNotification	电源插座状态通知：1=Active、0=Inactive。
powerOutletNotification	电源板设备插座状态通知。
rebootCompleted	KX II-101 已完成重新引导。
rebootStarted	KX II-101 已开始采用系统循环加电或操作系统热重新引导方式重新引导。
securityViolation	安全冲突。
startCCManagement	设备已被置于 CommandCenter 管理之下。
stopCCManagement	设备不再受 CommandCenter 管理。
userAdded	用户已被添加到系统中。
userAuthenticationFailure	用户尝试用错误用户名和/或密码登录。
userConnectionLost	有活动会话的用户发生异常会话终止。
userDeleted	用户帐号已被删除。
userLogin	用户已成功登录 KX II-101，已通过验证。
userLogout	用户成功注销 KX II-101。
userModified	用户帐号已被修改。
userPasswordChanged	如果修改该设备的任何用户的密码，均触发此事件。
userSessionTimeout	有活动会话的用户由于超时，造成会话终止。
vmImageConnected	用户尝试用虚拟介质功能在目标上加载设备或映像。针对对设备/映像映射（加载）进行的每次尝试，都生成此事件。

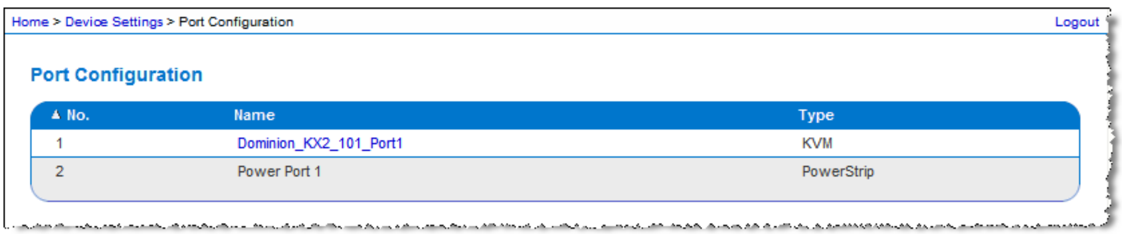
陷阱名称	说明
vmImageDisconnected	用户尝试用虚拟介质功能卸载目标上的设备或映像。

端口配置

Port Configuration（端口配置）页显示 KX II-101 端口列表。与 KVM 目标服务器或电源板相连的端口用蓝色显示，可以编辑。

➢ *更改端口配置：*

1. 选择 Device Settings（设备设置）> Port Configuration（端口配置）。打开 Port Configuration（端口配置）页：



本页最初按端口号顺序显示，但可以单击列标题，按任何字段排序。

- Port Number（端口号）。KX II-101 可用端口总数从 1 开始的编号。
- Port Name（端口名称）。给端口指定的名称。如果端口名称用空白显示，表示端口名称不能更改，端口不能编辑；用蓝色显示的端口名称可以编辑。

注意：不要在端口名称中使用撇号(')。

- Port Type（端口类型）。与端口相连的目标的类型：

端口类型	说明
PowerStrip（电源板）	电源板
KVM	KVM 目标

2. 单击要编辑的端口的 Port Name（端口名称）。
   - 对于 KVM 端口，打开 Port（端口）页。可以在本页上命名端口，创建电源关联，设置目标服务器设置。
   - 对于电源板，打开 power strips（电源板）页。可以在本页上命名电源板及其插座。

注意：只有在 Raritan 电源板连接 KX II-101 并正确配置之后，才启用 Power Port 1（电源端口 1）连接。否则，该连接被禁用。

9 电源控制

在本章内

概述

KX II-101 提供目标服务器远程电源控制。如要利用此功能，必须有一个 Raritan 远程电源板。

➢ *使用 KX II-101 电源控制功能：*

1. 连接电源板至目标服务器。
2. 命名电源板。
3. 使电源板插座与目标服务器关联。
4. 在 ***Powerstrip Device（电源板设备）*** (参看 "控制电源板设备" p. 130) 页上开关电源板上的插座。

连接电源板



1 从 KX II-101 到 Raritan 电源板所用的 DKX2-101-SPDUC 连接器（未画出）。

2 Raritan 电源板。

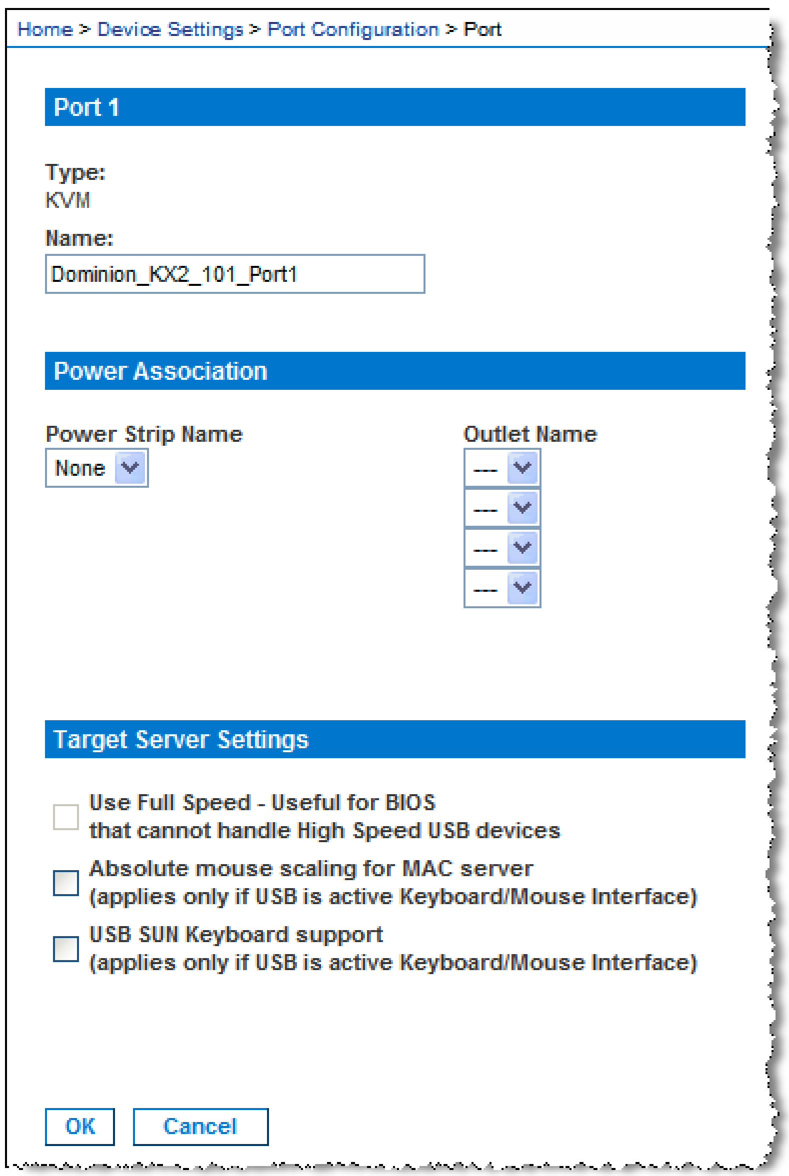
➢ *将 KX II-101 连接到 Raritan 电源板：*

1. 将 DKX2-101-SPDUC 电缆的 Mini DIM9M 连接器连接到 KX II-101 的 Admin（管理）端口。
2. 将 DKX2-101-SPDUC 电缆的 RJ45M 连接器连接到 Raritan 电源板上的串行端口连接器。
3. 用交流电源线的一端连接目标服务器，另一端连接电源板上的可用电源板插座。
4. 将电源板连接到交流电源。
5. 接通 Raritan 电源板电源。

命名电源板（电源板端口页）

在 Port Configuration（端口配置）页上选择与 Raritan 远程电源板相连的端口时，打开本 Port（端口）页。预先填充了 Type（类型）和 Name（名称）字段。显示电源板上每个插座的下列信息：插座 Number（编号）、Name（名称）和 Port Association（端口关联）。

用本页命名电源板及其插座；所有名称最长为 32 个字母数字字符，可以包含特殊字符。



注意：在使电源板与目标服务器（端口）关联时，插座名称被目标服务器名称替换掉（即使您给插座指定了另一个名称也是如此）。

➢ *命名电源板（和插座）：*

注意：CommandCenter Service Gateway 不识别有空格的电源板名称。

1. 将电源板 Name（名称）更改为便于记忆的名称。
2. 如果必要，更改（插座）Name（名称）。（插座名称默认为 Outlet # [插座编号]。）
3. 单击 OK（确定）。

➢ *取消而不保存更改：*

- 单击 Cancel（取消）。

使 KVM 目标服务器与插座关联（端口页）

在 Port Configuration（端口配置）页上选择与目标服务器相连的端口时，打开本 Port（端口）页。可以在本页上创建电源关联，将 Port Name（端口名称）更改为说明性更强的名称。

一台服务器最多可以有四个电源插头，您可以使它们与电源板关联。可以在本页上定义这些关联，以便在 Port Access（端口访问）页上如下所示接通服务器电源、断开服务器电源和给服务器循环加电。



*注意：如要使用此功能，必须给设备连接一个 Raritan Dominion PX 电源板。参看***连接电源板** *(p. 124)**部分了解详情。*

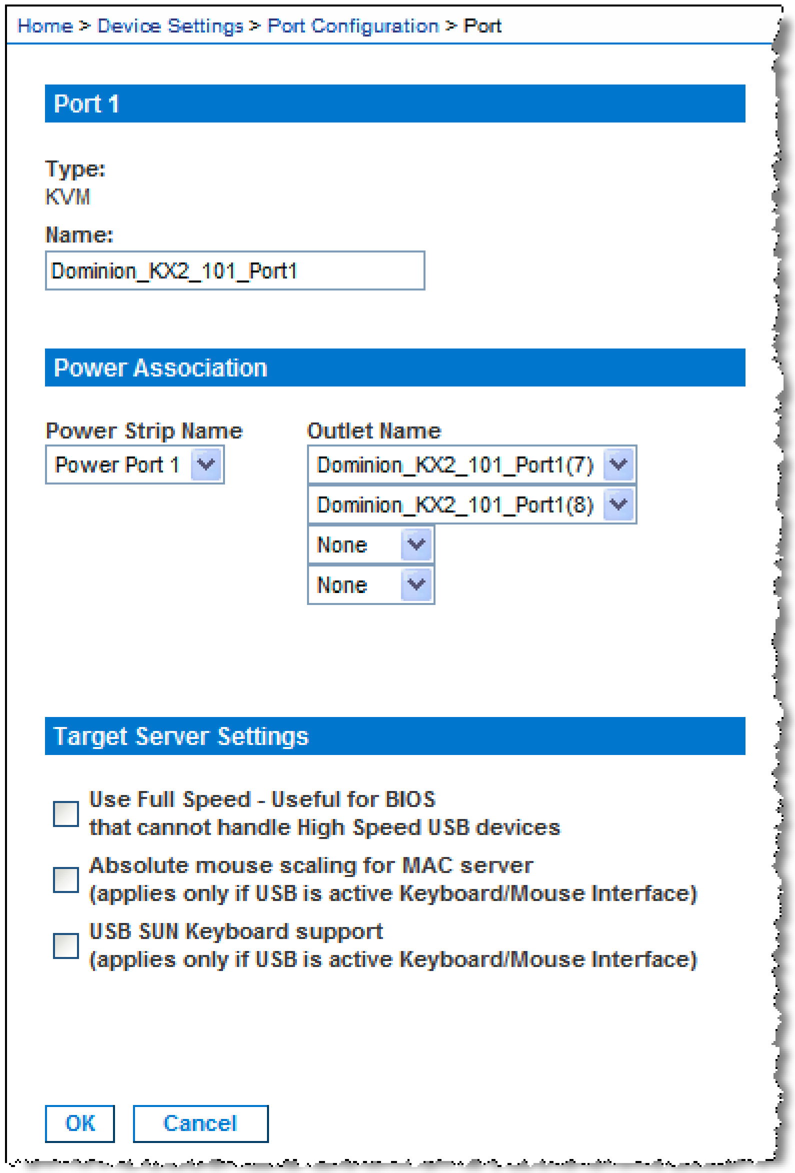
➢ *创建电源关联（使电源板插座与 KVM 目标服务器关联）：*

注意：在使电源板与目标服务器（端口）关联时，插座名称被端口名称替换掉。可以在 Port 2（端口 2）页上更改此名称。

1. 在 Power Strip Name（电源板名称）下拉列表上选择电源板。
2. 在 Outlet Name（插座名称）下拉列表上选择插座。

3. 针对每个希望的电源关联，重复步骤 1 和步骤 2。
4. 单击 OK（确定）。显示一条确认消息。

   下面说明有两个插座关联的电源板。



➢ *更改端口名称：*

1. 输入说明性名称，例如目标服务器的名称。名称最长为 32 个字母数字字符，可以包含特殊字符。
2. 单击 OK（确定）。

➢ *取消而不保存更改：*

- 单击 Cancel（取消）。

➢ *删除电源板关联：*

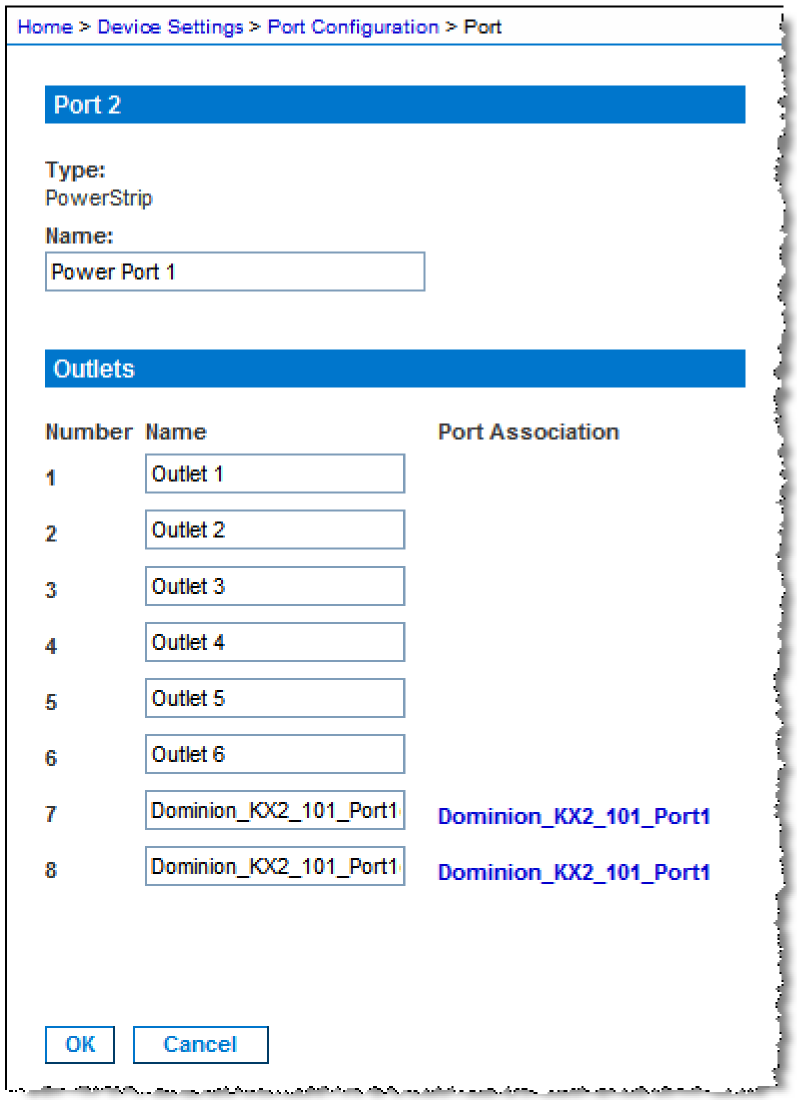
1. 在 Power Strip Name（电源板名称）下拉列表上选择适当的电源板。
2. 对于该电源板，在 Outlet Name（插座名称）下拉列表上选择适当的插座。
3. 在 Outlet Name（插座名称）下拉列表上选择 None（无）。
4. 单击 OK（确定）。电源板/插座关联被删除了。显示一条确认消息。

显示插座关联

➢ *显示电源端口配置：*

- 选择 Home（主页）> Device Settings（设备设置）> Port Configuration（端口配置）> [power port name（电源端口名称）]。

Outlets（插座）下面显示电源板插座关联。



➢ *编辑电源端口配置：*

- 编辑 Port 2（端口 2）> Name（名称）字段，即可更改电源端口名称。
- 编辑关联的 Outlets（插座）> Name（名称）字段，即可更改插座名称。Powerstrip Device（电源板设备）页显示插座名称。参看***控制电源板设备*** (p. 130)部分了解详情。
- 单击插座名称旁边的 Port Association（端口关联）链接并在 Port 1（端口 1）页上编辑它，即可更改插座关联。参看***使 KVM 目标服务器与插座关联（端口页）*** (p. 126)部分了解详情。

控制电源板设备

可以用 Powerstrip Device（电源板设备）页控制电源板设备。您可以用本页开关电源板上的每个插座。



➢ *控制与 KX II-101 相连的电源板：*

1. 选择 Home（主页）> Powerstrip（电源板）。

   打开 Powerstrip Device（电源板设备）页

2. 单击每个插座对应的 On（开）或 Off（关）按钮开关插座。
3. 在提示您确认选择时，单击 OK（确定）。

   接通或切断电源插座。

注意：KX II-101 只能控制一个电源板。不能在 Powerstrip（电源板）菜单上选择另一个电源板。

---

10 安全设置

在本章内

安全设置菜单

Security（安全）菜单按下列菜单项组织：Security Settings（安全设置）和 IP Access Control（IP 访问控制）。

使用：	目的：
Security Settings（安全设置）	配置登录限制、强密码、用户阻止、加密和共享等安全设置。
IP Access Control（IP 访问控制）	控制对 KX II-101 设备的访问。可以设置全局访问控制表，确保设备不响应来自被禁 IP 地址的数据包。

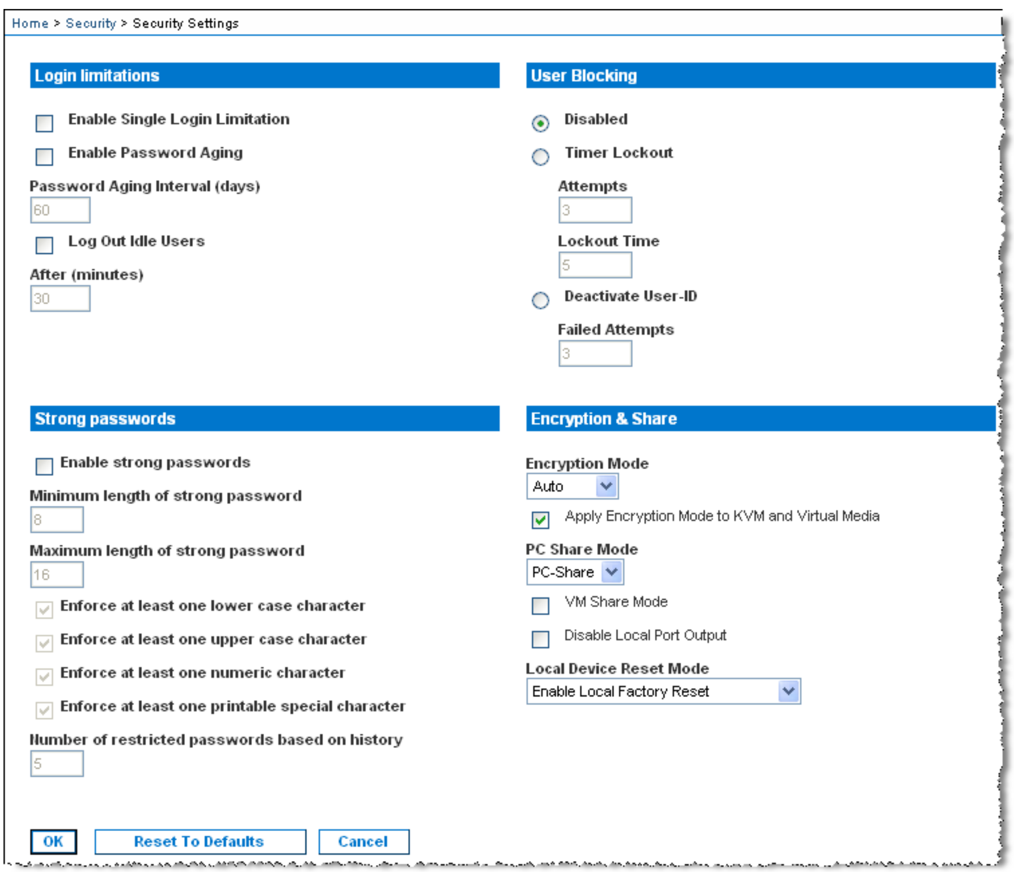
安全设置

可以在 Security Settings（安全设置）页上指定登录限制、用户阻止、密码规则、加密与共享。

Raritan SSL 证书用于公用密钥交换和专用密钥交换，并提供附加安全保护。Raritan Web 服务器证书是自签名证书；Java applet 证书用 VeriSign 证书签名。加密可以确保信息不会被窃听，这些证书确保您可以相信该实体就是 Raritan, Inc.。

➢ *配置安全设置：*

1. 选择 Security（安全）> Security Settings（安全设置）。打开 Security Settings（安全设置）页。



字段按下列组来组织：Login Limitations（登录限制）、Strong Passwords(强密码)、User Blocking(用户阻止)、Encryption & Share（加密和共享）。

2. 必要时更新***登录限制*** (p. 134)设置。
3. 必要时更新***强密码*** (p. 135)设置。

4. 必要时更新*用户阻止* (p. 136)设置。
5. 必要时更新加密和共享设置。
6. 单击 OK（确定）。

➢ *关闭本页但不保存任何更改：*

- 单击 Cancel（取消）。

➢ *恢复默认值：*

- 单击 Reset to Defaults（恢复默认值）。

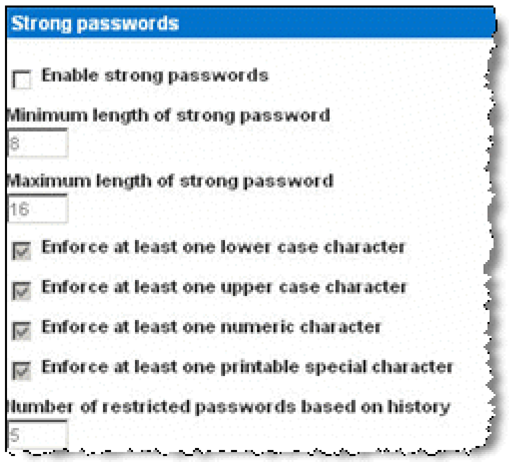
登录限制

可以用 Login Limitations（登录限制）页指定单点登录、密码有效期和空闲用户注销等限制。

限制	说明
Enable Single Login Limitation（启用单点登录限制）	在选择此选项之后，每个用户名在任何情况下只能登录一次。在取消选择此选项之后，可以在多个客户机工作站上用一个给定用户名/密码组合同时登录到设备上。
Enable Password Aging（启用密码有效期）	在选择此选项之后，所有用户必须根据在 Password Aging Interval（密码有效期）字段里指定的天数，定期更改自己的密码。 Password Aging Interval (days)（密码有效期[天]）。在选择 Enable Password Aging（启用密码有效期）复选框时，启用此字段，这是必需的。输入要在多少天之后更改密码。默认值是 60 天。
Log Out Idle Users（注销空闲用户）	如果选择此复选框，在经过一定的闲置时间之后，自动断开用户会话。在 After（之后）字段里输入时间量。如果没有键盘活动或鼠标活动，所有会话和所有资源均被注销。但如果正在进行虚拟介质会话，会话不会超时。 After (minutes)（之后[分钟]）。用户在被注销之前空闲的时间(分钟)。在选择 Log Out Idle Users（注销空闲用户）选项时，启用此字段。

强密码

强密码给系统提供更安全的本地验证。可以用 Strong Passwords（强密码）页指定密码标准，用于定义有效 KX II-101 本地密码的格式，例如最小长度、最大长度、所需的字符和密码历史记录保留天数。

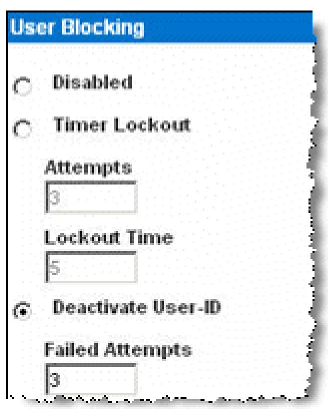


- Enable strong passwords（启用强密码）。强密码要求用户创建的密码至少有 8 个字符，其中至少有一个字母字符和一个非字母字符（标点字符或数字）。此外，密码和用户名的前 4 个字符不能相同。
  在选择此选项之后，执行强密码规则。凡是密码不符合强密码标准要求的用户，都要在下次登录时更改自己的密码。在取消选择此选项之后，仅执行标准格式验证。在选择此选项之后，启用下列必需的字段：
  - Minimum length of strong password（强密码最小长度）。密码至少有 8 个字符。默认值是 8 个字符，最多 63 个字符。
  - Maximum length of strong password（强密码最大长度）。默认值是 16 个字符，最多 64 个字符。
  - Enforce at least one lower case characte（强制至少有一个小写字符）。在选择此选项之后，要求密码至少有一个小写字符。
  - Enforce at least one upper case character（强制至少有一个大写字符）。在选择此选项之后，要求密码至少有一个大写字符。
  - Enforce at least one numeric character（强制至少有一个数字字符）。在选择此选项之后，要求密码至少有一个数字字符。
  - Enforce at least one printable special character（强制至少有一个可打印特殊字符）。在选择此选项之后，要求密码至少有一个（可打印的）特殊字符。
  - Number of restricted passwords based on history（根据历史记录限制的密码数）。此字段表示密码历史记录深度，即不能重复使用的旧密码数。范围是 1-12，默认值是 5。

用户阻止

User Blocking（用户阻止）选项指定在登录尝试失败次数达到限制次数之后，按什么标准阻止用户访问系统。下列三个选项是互斥的：

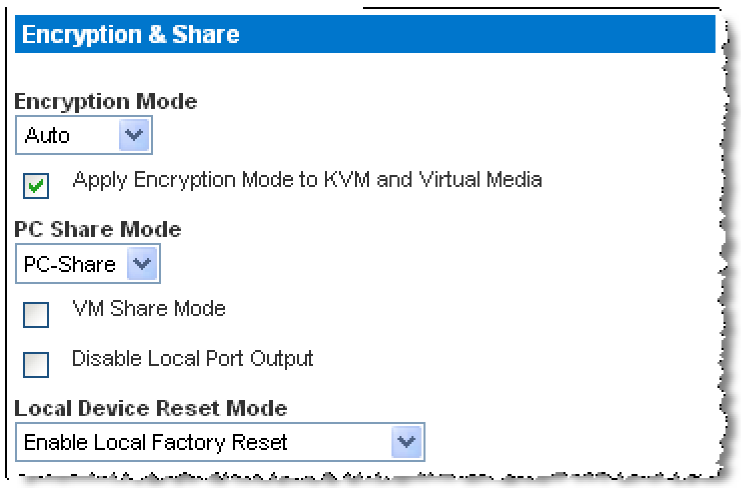
- Disabled（禁用）。默认选项；无论用户验证失败多少次，都不阻止该用户。
- Timer Lockout（定时器锁定）。在超过指定的登录尝试失败次数之后，在指定时间内拒绝用户访问系统。在选择此选项之后，启用下列字段：
  - Attempts（尝试次数）。在锁定用户之前的登录尝试失败次数。有效范围是 1 – 10，默认尝试次数是 3 次。
  - Lockout Time（锁定时间）。用户被锁定的时间长度。有效范围是 1 – 1440 分钟，默认值是 5 分钟。
- Deactivate User-ID（停用用户 ID）。在选择此选项之后，指定在达到 Failed Attempts（失败尝试次数）字段指定的登录尝试失败次数之后，用户不能访问系统：
  - Failed Attempts（失败尝试次数）。用户 ID 被停用之前的登录尝试失败次数。在选择 Deactivate User-ID（停用用户 ID）选项时，启用此字段。有效范围是 1 – 10。



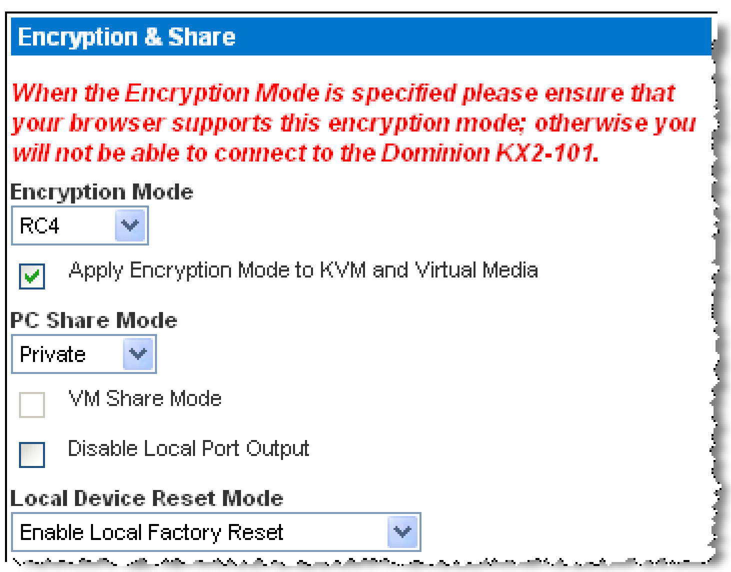
如果一个用户 ID 在指定的失败尝试次数之后被停用，管理员必须在 ***User（用户）*** (参看 "添加新用户" p. 46)页上更改该用户的密码，并选择 Active（活动）复选框激活该用户帐户。

加密和共享

可以用 Encryption & Share（加密和共享）设置来指定所用的加密类型、PC 共享模式、VM 共享模式、在按 KX II-101 复位按钮时要执行的复位的类型。



- Encryption Mode（加密模式）。在下拉列表上选择其中一个选项。在选择加密模式时，将显示一条警告：如果浏览器不支持所选的模式，将不能连接 KX II-101：



  - Auto（自动）。这是建议的选项；KX II-101 自动协商到可能的最高级加密。

- RC4。用 RSA RC4 加密方法保护用户名、密码和 KVM 数据，包括视频传输。这是 128 位 Secure Sockets Layer (SSL) 协议，在初次验证连接期间，它在 KX II-101 设备和远程 PC 之间提供专用通信通道。
- AES-128。Advanced Encryption Standard (AES) 是美国国家标准与技术研究院制定的电子数据加密规范，128 表示密钥长度。在指定 AES-128 时，确保自己的浏览器支持该规范，否则不能建立连接。参看***检查浏览器是否支持 AES 加密*** (p. 139)部分了解详情。
- AES-256。Advanced Encryption Standard (AES) 是美国国家标准与技术研究院制定的电子数据加密规范，256 表示密钥长度。在指定 AES-256 时，确保自己的浏览器支持该规范，否则不能建立连接。参看***检查浏览器是否支持 AES 加密*** (p. 139)部分了解详情。

- Apply Encryption Mode to KVM and Virtual Media（将加密模式应用于 KVM 和虚拟介质）。在选择此选项之后，将所选的加密模式应用于 KVM 和虚拟介质。在验证之后，KVM 数据和虚拟介质数据也采用 128 位加密方法传输。
- PC Share Mode（PC 共享模式）。确定全局并发远程 KVM 访问，最多允许八个远程用户同时登录到一台 KX II-101，可通过该设备同时查看和控制同一个目标服务器。单击下拉列表选择下列选项之一：
  - Private（专用）：禁止 PC 共享，这是默认模式。每个目标服务器每次只能供一个用户以独占方式访问。
  - PC-Share（PC 共享）：KVM 目标服务器每次最多可供八个用户（管理员或非管理员）访问。每个远程用户有同等的键盘和鼠标控制权，但要注意假如一个用户不停止输入或移动鼠标，会出现控制权不均现象。
- VM Share Mode（VM 共享模式）。仅当启用 PC-Share Mode（PC 共享模式）时，才启用此选项。在选择此选项之后，允许多个用户共享虚拟介质，即几个用户可以访问同一个虚拟介质会话。在默认情况下禁用此选项。
- Local Device Reset Mode（本地设备复位模式）。此选项指定在按（设备背面的）硬件复位按钮时，要执行哪些操作。如要了解详情，参看复位按钮。选择下列选项之一：
  - Enable Local Factory Reset (Default)（启用本地出厂复位[默认值]）。使 KX II-101 设备恢复到出厂默认值。
  - Enable Local Admin Password Reset（启用本地管理员密码复位）。仅复位本地管理员密码。密码复位为 raritan。
  - Disable All Local Resets（禁用所有本地复位）。不执行任何复位操作。

检查浏览器是否支持 AES 加密

如果不知道浏览器是否使用 AES，可以向浏览器开发商咨询，或者用浏览器打开 https://www.fortify.net/sslcheck.html 网站，检查它是否支持此加密方法。本网站检测浏览器使用的加密方法，并显示检测报告。

注意：IE6 不支持 AES 128 位或 256 位加密。

AES 256 先决条件和支持的配置

只有下列网络浏览器支持 AES 256 位加密：

- Firefox 2.0.0.7
- Mozilla 1.7.13
- Internet Explorer 7

除了浏览器支持，AES 256 还要求安装 Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files。

供各种 JRE 使用的 Jurisdiction 策略文件可以在下列链接的 other downloads（其他下载）部分下载：

- JRE1.4.2 - http://java.sun.com/j2se/1.4.2/download.html
- JRE1.5 - http://java.sun.com/javase/downloads/index_jdk5.jsp

IP 访问控制

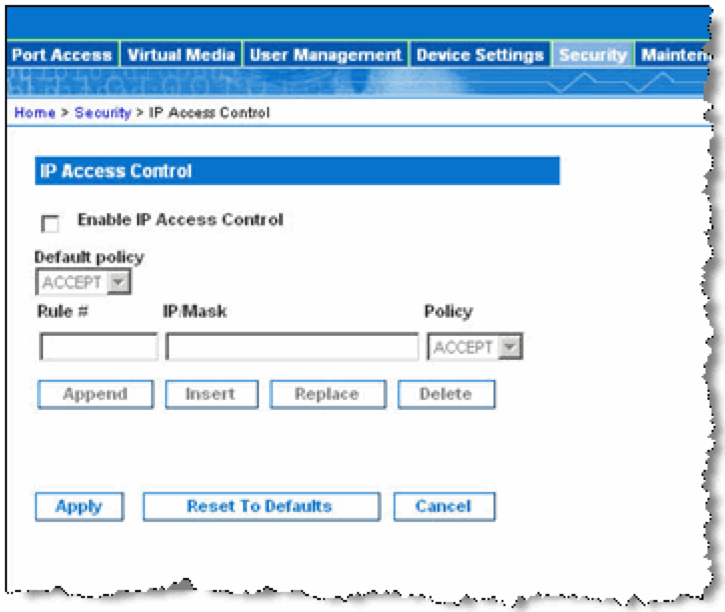
可以用 IP Access Control（IP 访问控制）页控制对 KX II-101 设备的访问。设置全局访问控制表 (ACL)，确保设备不响应来自被禁 IP 地址的数据包。IP Access Control（IP 访问控制）是全局性的，影响整个 KX II-101 设备，但您也可以在组一级控制设备访问。参看基于组的 IP 访问控制部分了解组控制。

重要事项：KX II-101 本地端口使用 IP 地址 127.0.0.1。在创建 IP 访问控制表时，如果 127.0.0.1 处于被禁 IP 地址范围内，您将不能访问 KX II-101 本地端口。

➢ *使用 IP 访问控制：*

1. 用下列方法之一打开 IP Access Control（IP 访问控制）页：
   - 选择 Security（安全）> IP Access Control（IP 访问控制），或者
   - 单击 Network Settings（网络设置）页上的 Set System ACL（设置系统 ACL）按钮

打开 IP Access Control（IP 访问控制）页。



2. 选择 Enable IP Access Control（启用 IP 访问控制）复选框，从而启用 IP 访问控制和本页上的其余字段。
3. 选择 Default Policy（默认策略）。这是针对那些不在指定范围内的 IP 地址执行的操作。
   - Accept（接受）。允许 IP 地址访问 KX II-101 设备。
   - Drop（放弃）。拒绝 IP 地址访问 KX II-101 设备。

➢ *添加（附加）规则：*

1. 在 IP/Mask（IP/掩码）字段里输入 IP 地址和子网掩码。
2. 在 Policy（策略）下拉列表上选择策略。
3. 单击 Append（附加）。规则被添加到规则列表的底部。
4. 对于要输入的每个规则，重复步骤 1 到步骤 3。

➢ *插入规则：*

1. 输入 Rule #（规则号）。在使用 Insert（插入）命令时，需要填写 Rule #（规则号）。
2. 在 IP/Mask（IP/掩码）字段里输入 IP 地址和子网掩码。
3. 在 Policy（策略）下拉列表上选择策略。
4. 单击 Insert（插入）。如果刚才输入的 Rule #（规则号）与现有 Rule #（规则号），新规则将放在现有规则的前面，列表上的所有规则均向下移动。

➢ *替换规则：*

1. 指定要替换的 Rule #（规则号）。
2. 在 IP/Mask（IP/掩码）字段里输入 IP 地址和子网掩码。
3. 在 Policy（策略）下拉列表上选择策略。
4. 单击 Replace（替换）。新规则替换有相同 Rule #（规则号）的原始规则。

➢ *删除规则：*

1. 指定要删除的 Rule #（规则号）。
2. 单击 Delete（删除）。
3. 系统提示您确认删除。单击 OK（确定）。

提示：规则号便于您更好地控制规则创建顺序。

---

11 维护

在本章内

维护菜单

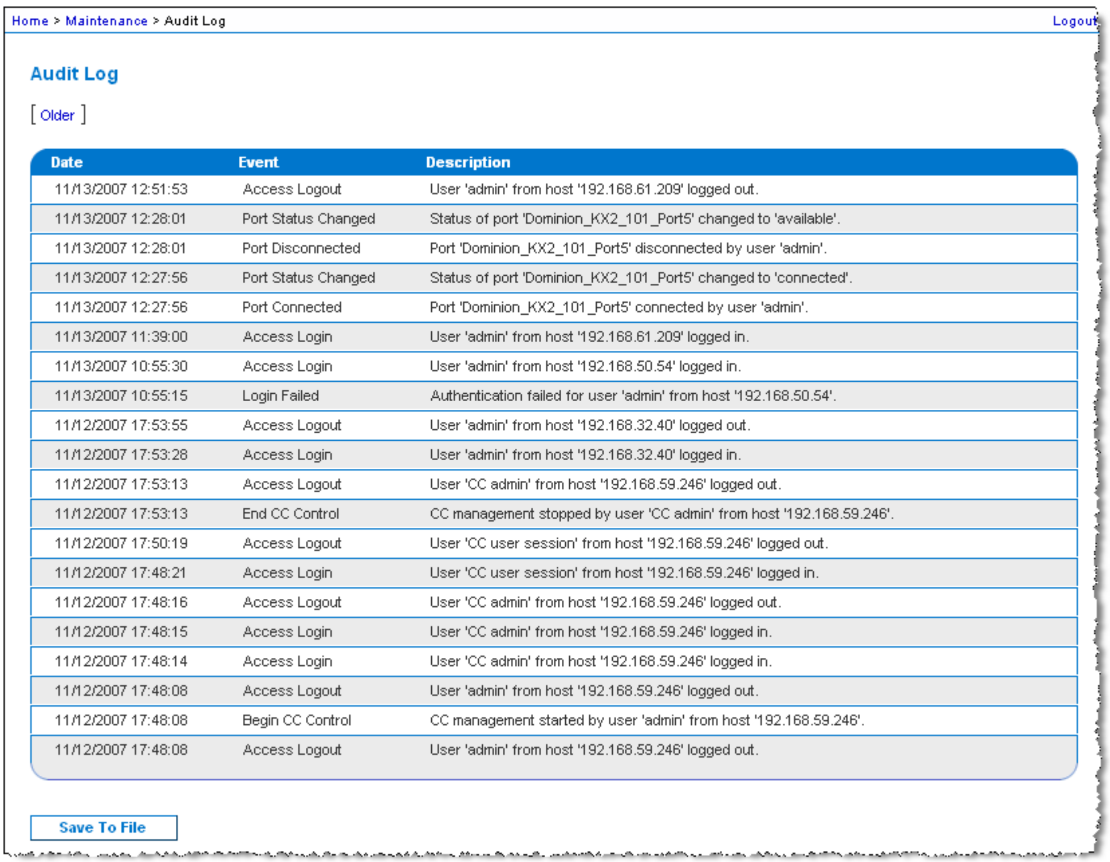
Maintenance（维护）菜单包括这些选项：Audit Log（审计日志）、Device Information（设备信息）、Backup/Restore（备份/恢复）、Firmware Upgrade（固件升级）、Factory Reset（出厂复位）、Upgrade History（升级历史记录）和 Reboot（重新引导）。

审计日志

针对 KX II-101 系统事件创建的日志。

➢ *查看 KX II-101 设备的审计日志：*

1. 选择 Maintenance（维护）> Audit Log（审计日志）。打开 Audit Log（审计日志）页：



Date	Event	Description
11/13/2007 12:51:53	Access Logout	User 'admin' from host '192.168.61.209' logged out.
11/13/2007 12:28:01	Port Status Changed	Status of port 'Dominion_KX2_101_Port5' changed to 'available'.
11/13/2007 12:28:01	Port Disconnected	Port 'Dominion_KX2_101_Port5' disconnected by user 'admin'.
11/13/2007 12:27:56	Port Status Changed	Status of port 'Dominion_KX2_101_Port5' changed to 'connected'.
11/13/2007 12:27:56	Port Connected	Port 'Dominion_KX2_101_Port5' connected by user 'admin'.
11/13/2007 11:39:00	Access Login	User 'admin' from host '192.168.61.209' logged in.
11/13/2007 10:55:30	Access Login	User 'admin' from host '192.168.50.54' logged in.
11/13/2007 10:55:15	Login Failed	Authentication failed for user 'admin' from host '192.168.50.54'.
11/12/2007 17:53:55	Access Logout	User 'admin' from host '192.168.32.40' logged out.
11/12/2007 17:53:28	Access Login	User 'admin' from host '192.168.32.40' logged in.
11/12/2007 17:53:13	Access Logout	User 'CC admin' from host '192.168.59.246' logged out.
11/12/2007 17:53:13	End CC Control	CC management stopped by user 'CC admin' from host '192.168.59.246'.
11/12/2007 17:50:19	Access Logout	User 'CC user session' from host '192.168.59.246' logged out.
11/12/2007 17:48:21	Access Login	User 'CC user session' from host '192.168.59.246' logged in.
11/12/2007 17:48:16	Access Logout	User 'CC admin' from host '192.168.59.246' logged out.
11/12/2007 17:48:15	Access Login	User 'CC admin' from host '192.168.59.246' logged in.
11/12/2007 17:48:14	Access Login	User 'CC admin' from host '192.168.59.246' logged in.
11/12/2007 17:48:08	Access Logout	User 'admin' from host '192.168.59.246' logged out.
11/12/2007 17:48:08	Begin CC Control	CC management started by user 'admin' from host '192.168.59.246'.
11/12/2007 17:48:08	Access Logout	User 'admin' from host '192.168.59.246' logged out.

Audit Log（审计日志）页按日期和时间显示事件（最近的事件在前面）。审计日志提供下列信息：

- Date（日期）。事件发生的日期和时间（24 小时制）。
- Event（事件）。Event Management（事件管理）页列出的事件名称。
- Description（说明）。详细事件说明。

➢ *保存审计日志：*

注意：审计日志保存操作只能在 KX II-101 Remote Console 上执行，不能在本地控制台上执行。

1. 单击 Save to File（保存到文件）按钮。打开 Save File（保存文件）对话框。
2. 选择文件名和文件保存位置，单击 Save（保存）。审计日志用指定的名称和位置保存在本地客户机上。

➢ *遍历审计日志：*

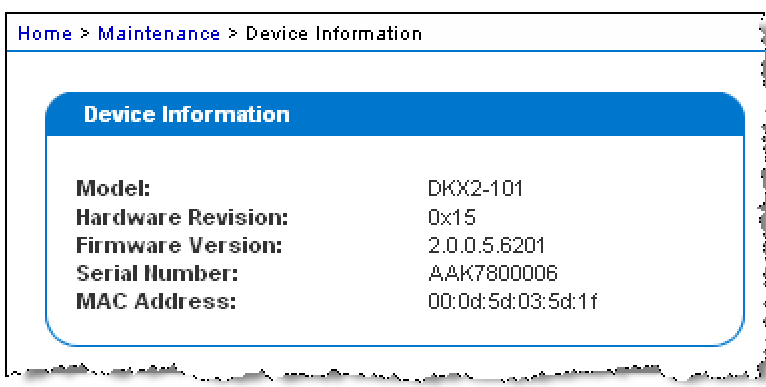
- 使用 [Older]（较旧）和 [Newer]（较新）链接。

设备信息

Device Information（设备信息）页显示有关 KX II-101 设备的详细信息。在需要与 Raritan 技术支持部门联系时，此信息很有用。

➢ *查看有关 KX II-101 的信息：*

- 选择 Maintenance（维护）> Device Information（设备信息）。打开 Device Information（设备信息）页：



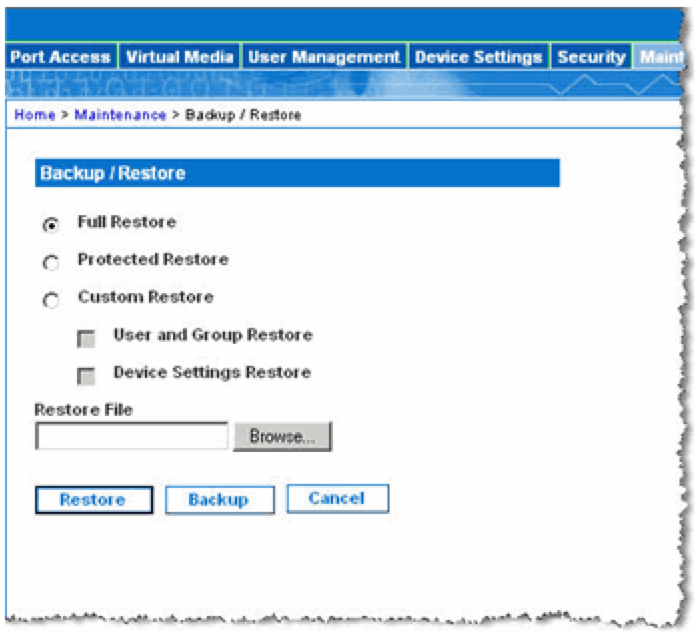
显示有关 KX II-101 的下列信息：Model（型号）、Hardware Revision（硬件修订版）、Firmware Version（固件版本）、Serial Number（序列号）和 MAC Address（MAC 地址）。

备份和恢复

可以在 Backup/Restore（备份/恢复）页上备份和恢复 KX II-101 的设置和配置。备份和恢复功能除了用于使业务保持连续不断，还可以节省时间。例如可以备份在一台 KX II-101 上使用的配置设置，在另一台 KX II-101 上恢复这些配置，快速给使用新 KX II-101 的团队提供访问。还可以先设置一台 KX II-101，然后将其配置复制到多台 KX II-101 设备上。

➢ *访问 Backup/Restore（备份/恢复）页：*

- 选择 Maintenance（维护）> Backup/Restore（备份/恢复）。打开 Backup/Restore（备份/恢复）页。



注意：备份功能始终进行完整系统备份。恢复可以是完整恢复，也可以是部分恢复，任您选择。

➢ *备份 KX II-101：*

1. 单击 Backup（备份）。打开 File Download（文件下载）对话框。
2. 单击 Save（保存）。打开 Save As（另存为）对话框。
3. 选择保存位置，指定文件名，然后单击 Save（保存）。打开 Download Complete（下载完成）对话框。
4. 单击 Close（关闭）。备份文件用指定的名称和位置保存到本地客户机上。

➢ *恢复 KX II-101：*

警告：在将 KX II-101 恢复到旧版本时，要小心谨慎。在恢复备份文件时，必须知道用户名和密码。如果忘了旧的管理用户名和密码，不能恢复 KX II-101。

此外，如果在备份时使用了不同的 IP 地址，该 IP 地址也将被恢复。如果该配置使用 DHCP，只有在您有权访问本地端口检查更新后的 IP 地址时，才可能需要执行此操作。

1. 选择要运行的恢复的类型：
   - Full Restore（全恢复）。完整恢复整个系统，通常用于进行传统备份和恢复。
   - Protected Restore（受保护的恢复）。除了序列号、MAC 地址、IP 地址、名称等设备特定的信息，恢复其他所有数据。在选择此选项之后，可以先设置一台 KX II-101，然后将其配置复制到多台 KX II-101 设备上。
   - Custom Restore（定制恢复）。在选择此选项之后，可以选择 User and Group Restore（用户和组恢复）和/或 Device Settings Restore（设备设置恢复）。选择相应的复选框：
     - User and Group Restore（用户和组恢复）。此选项仅包括用户和组信息。用此选项在另一台 KX II-101 上快速设置用户。
     - Device Settings Restore（设备配置恢复）。此选项仅包括设备设置。用此选项快速复制设备信息。
2. 单击 Browse（浏览）按钮。打开 Choose file（选择文件）对话框。
3. 找到并选择相应的备份文件，然后单击 Open（打开）。Restore File（恢复文件）字段列出所选的文件。
4. 单击 Restore（恢复）。根据所选的恢复类型恢复配置。

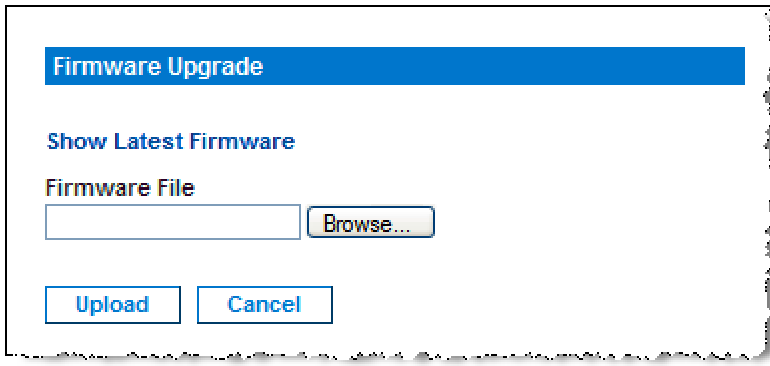
固件升级

用 Firmware Upgrade（固件升级）页升级 KX II-101 设备的固件。本页只能在 KX II-101 Remote Console 上使用。

重要事项：在升级过程中，不要断开 KX II-101 设备电源，否则很可能会损坏设备。

- *升级 KX II-101 设备：*

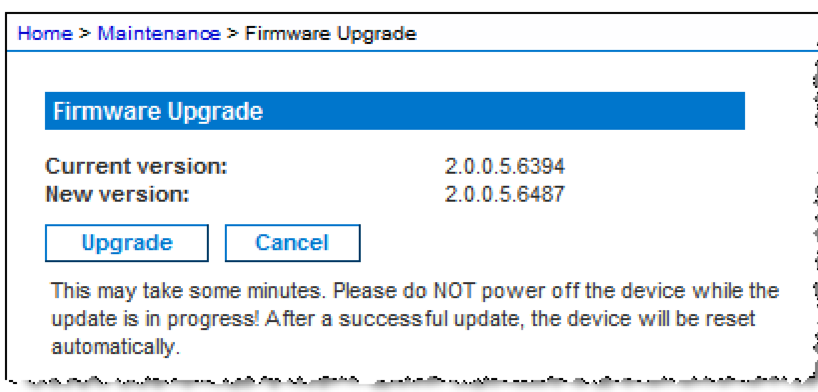
1. 选择 Maintenance（维护）> Firmware Upgrade（固件升级）。打开 Firmware Upgrade（固件升级）页：



2. 单击 Firmware Upgrades（固件升级）> KX II-101 页上的 Show Latest Firmware（显示最新固件）链接，找到相应的 Raritan 固件分发文件 (*.RFP)，并下载该文件。
3. 解压升级文件，仔细阅读固件 ZIP 文件包含的所有说明，然后升级固件。

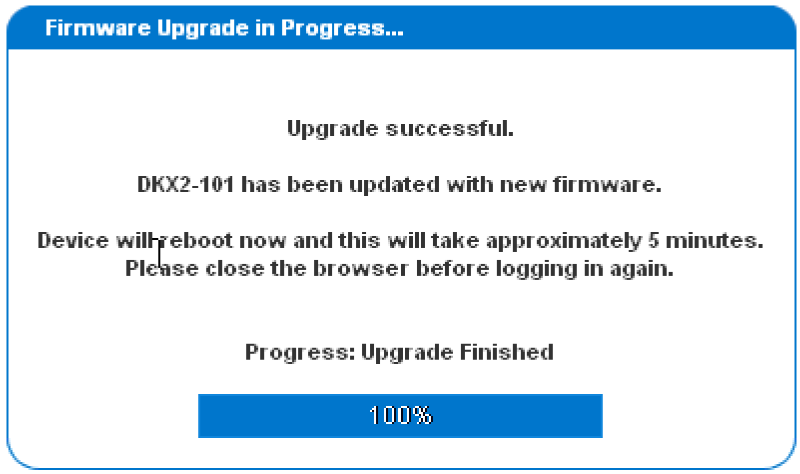
注意：在上载之前，将固件更新文件复制到本地 PC。不要从网络驱动器上加载文件。单击 Browse（浏览）按钮找到要解压升级文件的目录。

4. 单击 Firmware Upgrade（固件升级）页上的 Upload（上载）。显示有关升级和版本号的信息，需要您确认：



注意：此时注销已连接的用户，禁止新的登录尝试。

5. 单击 Upgrade（升级）。等待升级完成。在升级过程中，显示状态信息和进度条。在完成升级之后，设备重新引导。



6. 根据提示关闭浏览器，等待大约 5 分钟后再次登录到 KX II-101。

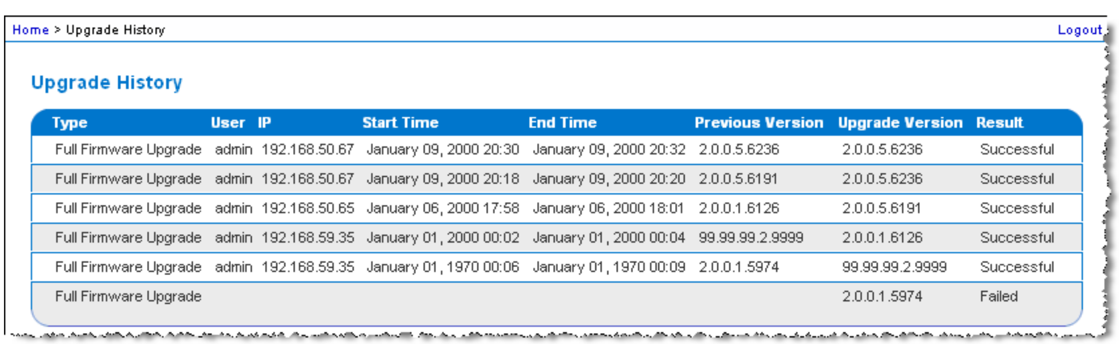
如要了解在使用 Multi-Platform Client 时如何升级设备固件，参看《Raritan Multi-Platform Client (MPC) 用户指南》。

升级历史记录

KX II-101 提供有关在 KX II-101 设备和相连的 CIM 上执行的升级的信息。

➢ *查看升级历史记录：*

- 选择 Maintenance（维护）> Upgrade History（升级历史记录）。打开 Upgrade History（升级历史记录）页：



Type	User	IP	Start Time	End Time	Previous Version	Upgrade Version	Result
Full Firmware Upgrade	admin	192.168.50.67	January 09, 2000 20:30	January 09, 2000 20:32	2.0.0.5.6236	2.0.0.5.6236	Successful
Full Firmware Upgrade	admin	192.168.50.67	January 09, 2000 20:18	January 09, 2000 20:20	2.0.0.5.6191	2.0.0.5.6236	Successful
Full Firmware Upgrade	admin	192.168.50.65	January 06, 2000 17:58	January 06, 2000 18:01	2.0.0.1.6126	2.0.0.5.6191	Successful
Full Firmware Upgrade	admin	192.168.59.35	January 01, 2000 00:02	January 01, 2000 00:04	99.99.99.2.9999	2.0.0.1.6126	Successful
Full Firmware Upgrade	admin	192.168.59.35	January 01, 1970 00:06	January 01, 1970 00:09	2.0.0.1.5974	99.99.99.2.9999	Successful
Full Firmware Upgrade						2.0.0.1.5974	Failed

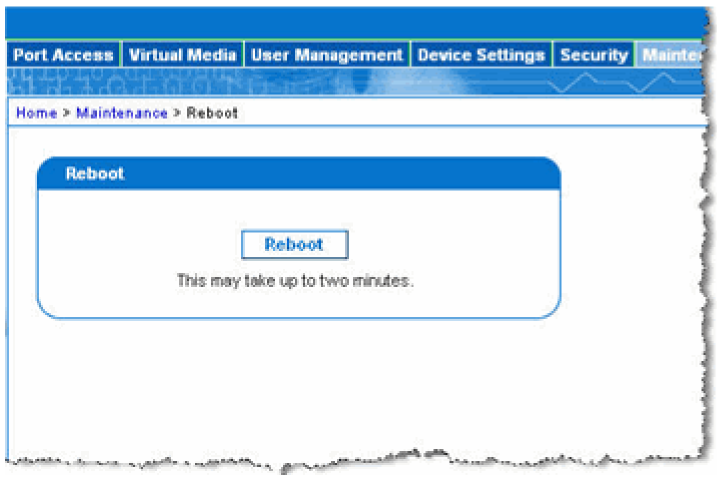
重新引导

Reboot（重新引导）页提供一种安全的受控方法来重新引导 KX II-101 设备，这是建议的重新引导方法。

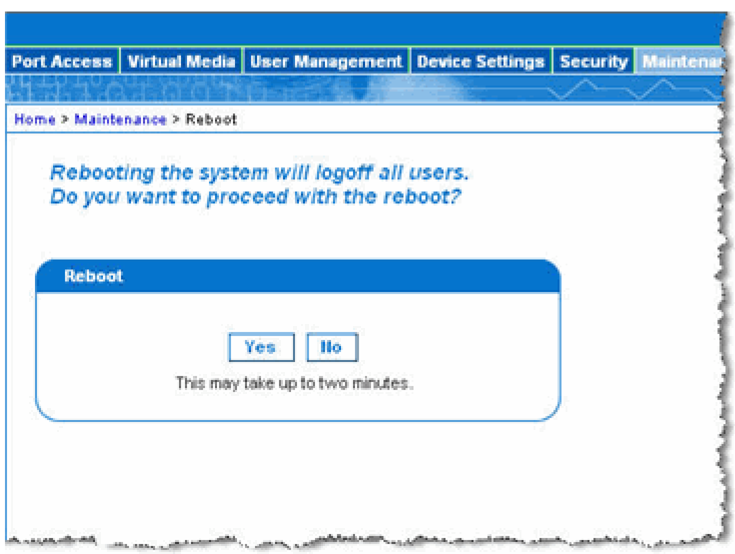
重要事项：所有 KVM 连接和串行连接将被关闭，所有用户将被注销。

➤ *重新引导 KX II-101：*

1. 选择 Maintenance（维护）> Reboot（重新引导）。打开 Reboot（重新引导）页。



2. 单击 Reboot（重新引导）按钮。系统提示您确认该操作。



3. 单击 Yes（是）按钮继续重新引导。

➢ *退出而不重新引导：*

- 单击 No（否）。

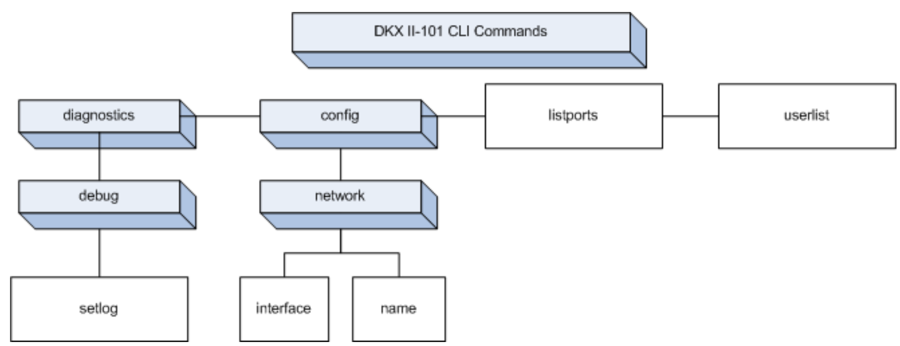
12 命令行界面

在本章内

概述

本章概述可与 KX II-101 一起使用的命令行界面命令。参看***命令行界面命令*** (p. 155)了解命令列表和命令定义，以及至本章（有命令示例的）各节的链接。

下图概述命令行命令：



注意：可以在各级命令行界面到上图所示的界面上使用下列常用命令：top、history、logout、quit 和 help。

用命令行界面访问 KX II-101

用下列方法之一访问 KX II-101：

- 基于 IP 连接的 TELNET
- 基于 IP 连接的 SSH (Secure Shell)
- 通过电缆连接的 RS-232 串行接口和 HyperTerminal 等终端仿真程序的多功能管理串行端口

可以使用许多 SSH/TELNET 客户机，这些客户机可以在下列网址下载：

- Putty — ***http://www.chiark.greenend.org.uk/~sgtatham/putty/*** http://www.chiark.greenend.org.uk/~sgtatham/putty/
- ssh.com 的 SSH Client — ***www.ssh.com*** http://www.ssh.com
- Applet SSH Client — ***www.netspace.org/ssh*** http://www.netspace.org/ssh
- OpenSSH Client — ***www.openssh.org*** http://www.openssh.org

*注意：在用 SSH 或 TELNET 访问命令行界面时，要求您在 KX II-101 Remote Client 的 Device Services（设备服务）页上设置访问权。参看***设备服务*** *(p. 110)部分了解详情。*

用 SSH 连接 KX II-101

用支持 SSHv2 的任何 SSH 客户机连接 KX II-101。必须在 Device Services（设备服务）页上启用 SSH 访问。参看***设备服务*** (p. 110)部分了解详情。

注意：为安全起见，KX II-101 不支持 SSH V1 连接。

Windows PC 上的 SSH 访问

➢ *在 Windows PC 上打开 SSH 会话：*

1. 启动 SSH 客户端软件，例如 PuTTY。
2. 输入 KX II-101 服务器的 IP 地址 192.168.0.192。
3. 选择 SSH，它使用默认配置端口 22。
4. 单击 Open（打开）按钮。
5. 显示下列提示：
   `login as`（登录为）:

参看登录部分了解登录信息。

UNIX 工作站上的 SSH 访问

➢ *如要在 UNIX 工作站上打开 SSH 会话并作为 admin 用户登录，输入下列命令：*

```
ssh -l admin 192.168.30.222
```

显示 Password（密码）提示符。

参看登录部分了解登录信息。

登录

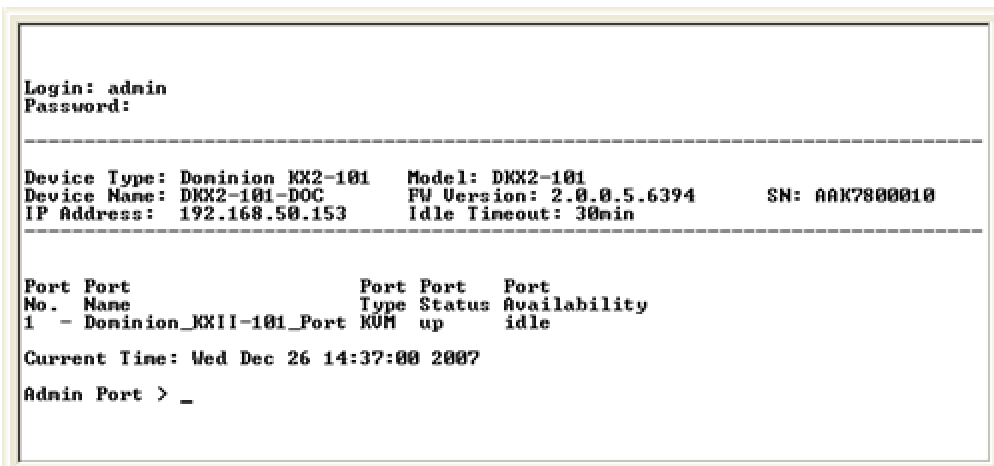
➢ *如要登录，如下输入用户名 admin：*

Login（登录）: admin

显示 Password（密码）提示符。输入默认密码：raritan

Password（密码）：

显示欢迎消息。现在可以作为管理员登录。



在阅读后面的***命令行界面导航*** (p. 153)一节之后，可以执行如***使用管理串行控制台*** (参看 "使用终端仿真程序" p. 24)所述的初始配置任务。

命令行界面导航

在使用命令行界面之前，必须了解命令行界面导航和语法。此外，还有可简化命令行界面使用的击键组合。

命令行界面提示

命令行界面提示表示当前命令级别。命令提示的根部分是登录名；对于使用终端仿真应用程序的直接管理串行端口，Admin Port（管理端口）是命令的根部分：

```
Admin Port > Config > Network >
```

对于 TELNET/SSH，admin（管理）是命令的根部分：

```
admin > config > network >
```

命令输入完成

命令行界面支持不完整的命令输入。在输入命令的前面几个字符之后，按 Tab 键；如果这些字符唯一匹配一个命令，命令行界面自动完成输入。

- 如果找不到匹配的命令，命令行界面显示该级对应的多个有效命令。
- 如果找到多个匹配的命令，命令行界面还显示这些有效命令。
- 接着输入后面的字符，使输入是唯一的，然后按 Tab 键完成输入。

命令行界面语法 — 提示和快捷键

提示

- 命令按字母顺序排列。
- 命令不区分大小写。
- 参数名称是单个词，没有下划线。
- 没有自变量的命令默认显示该命令对应的当前设置。
- 在命令后面输入问号 (?)，显示该命令的帮助。
- 竖线 (|) 表示一组可选的或要求的关键字或自变量内的选项。

快捷键

- 按向上箭头键显示上一个输入。
- 按 Backspace（退格）键删除上一个输入字符。
- 如果输入了错误参数，按 Ctrl/C 终止命令或取消命令。
- 按 Enter（确认）键执行命令。
- 按 Tab 键完成命令输入。例如 `Admin Port > Conf`，系统然后显示 `Admin Port > Config >` 提示。

所有命令行界面的常用命令

命令行界面命令列出可在所有命令行界面上执行的命令。这些命令也有助于说明命令行界面。

命令	说明
top	返回命令分层结构的顶部或 username 提示。
history	显示用户最近在 KX II-101 命令行界面上输入的 200 条命令。
help	显示命令行界面语法概述。
quit	让用户返回上一级。
logout	注销用户会话。

命令行界面命令

下表列出并说明所有可用的命令行界面命令。

命令	说明
config	切换到 Configuration（配置）菜单。
diagnostics (参看 "诊断" p. 156)	切换到 Diagnostics（诊断）菜单。
debug (参看 "调试" p. 156)	切换到 Debug（调式）菜单。
help	显示命令行界面语法概述。
history	显示当前会话的命令行历史记录。
interface	配置 KX II-101 网络接口。
listports (参看 "Listports 命令" p. 159)	列出端口、端口名称、端口类型、端口状态和端口可用性。
logout	注销当前命令行界面会话。
name (参看 "Name 命令" p. 158)	设置设备名称。
network (参看 "网络" p. 157)	显示网络配置，允许您配置网络设置。
quit	返回上一个命令。

setlog (参看 "Setlog 命令" p. 156)	设置设备日志记录选项。
top	返回根菜单。
userlist (参看 "Userlist 命令" p. 159)	列出活动用户数、用户名、端口和状态。

诊断

Diagnostics（诊断）菜单允许您给 KX II-101 的不同模块设置日志记录选项。只有在得到 Raritan 技术支持工程师的指示后，才应设置日志记录选项。这些日志记录选项使支持工程师能获得调试和排除故障所需的适当信息。在得到支持工程师的指示时，他/她会告诉您如何设置日志记录选项，如何生成日志文件并把它发送给 Raritan 技术支持部门。

重要事项：日志记录选项必须在 Raritan 技术支持工程师的监督下设置。

调试

Diagnostics（诊断）> Debug（调试）菜单允许您选择 Setlog 命令，给 KX II-101 设置日志记录选项。

Setlog 命令

Setlog 命令允许您给 KX II-101 的不同模块设置日志记录选项，查看每个模块的当前日志记录级别。setlog 命令语法如下：

```
setlog [module <module>] [level <level>] [vflag <vflag>]
[verbose <on|off>]

 Set/Get diag log level
```

Setlog 命令选项如下表所述。Raritan 技术支持部门会告诉您如何配置这些设置。

命令选项	说明
module	模块名称。
level	诊断级别： err（错误） warn（警告） info（信息） debug（调试） trace（跟踪）

命令选项	说明
vflag	verbose 标志类型： timestamp（时间戳） module（模块） thread（线程） fileline（文件行）
verbose [on|off]	开关 verbose 日志记录。

Setlog 命令示例

下列 Setlog 命令给 libpp_serial 模块设置对 verbose 登录进行调试所需的日志记录级别。

```
Setlog module libpp_serial level debug verbose on
```

配置

Configuration（配置）菜单允许您访问在配置网络接口并设置设备名称时所用的网络命令。

网络

Configuration（配置）> Network（网络）命令用于配置 KX II-101 网络连接和设备名称。

命令	说明
interface	配置 KX II-101 设备网络接口。
name	设置设备名称。

Name 命令

name 命令用于配置设备名称和主机名。

设备名称的语法如下：

```
name devicename<>
```

主机名的语法如下：

```
name hostname<>
```

name 命令示例

下列命令设置设备名称：

```
Admin Port > Config > Network > name devicename <device name>
```

下列命令设置主机名：

```
Admin Port > Config > Network > name hostname <host name>
```

Interface 命令

interface 命令用于配置 KX II-101 网络接口。如果该命令被接受，设备就断开 HTTP/HTTPS 连接，并初始化新网络连接。所有 HTTP/HTTPS 用户必须用新 IP 地址与正确的用户名和密码重新连接设备。参看***安装和配置*** (p. 7)部分了解详情。

interface 命令语法如下：

```
interface [ipauto <none|dhcp>] [ip <ipaddress>] [mask <subnetmask>] [gw <ipaddress>] [mode <auto/10hdx/10fdx/100hdx/100fdx]
```

网络命令选项如下表所述。

命令选项	说明
ipauto	静态或动态 IP 地址。
ip ipaddress	给 KX II-101 分配的 IP 地址，以便通过 IP 网络进行访问
mask subnetmask	IP 管理员提供的子网掩码。
gw ipaddress	IP 管理员提供的网关 IP 地址。
mode <auto | 100fdx>	将 Ethernet Mode 设置为自动检测或强制 100Mbps 全双工 (100fdx)

interface 命令示例

下列命令设置 IP 地址、掩码和网关地址，并将模式设置为自动检测。

```
Admin Port > Config > Network > interface ipauto none ip
192.168.50.12 mask 255.255.255.0 gw 192.168.51.12 mode
auto
```

Listports 命令

Listports 命令列出活动用户数、用户名、端口和状态。

Listports 命令示例

```
Admin Port > listports

Port Port                   Port Port   Port

No.  Name                   Type Status Availability

1  - Dominion_KXII-101_Port KVM  up     idle
```

Userlist 命令

Userlist 命令列出端口、端口名称、端口类型、端口状态和端口可用性。

Userlist 命令示例

```
Admin Port > Userlist

Active user number: 1

User Name | From       | Status

------------------------------------------------------
--

admin     | Admin Port | active
```

13 诊断

在本章内

诊断菜单

Diagnostics（诊断）页用于排除故障，主要供 KX II-101 设备管理员使用。所有 Diagnostics（诊断）页（Device Diagnostics [设备诊断]除外）均运行标准网络命令，显示的信息就是这些命令的输出。Diagnostics（诊断）菜单选项有助您调试和配置网络设置。

Device Diagnostics（设备诊断）选项应在 Raritan 技术支持部门的指导下使用。

有三个选项可供选择：

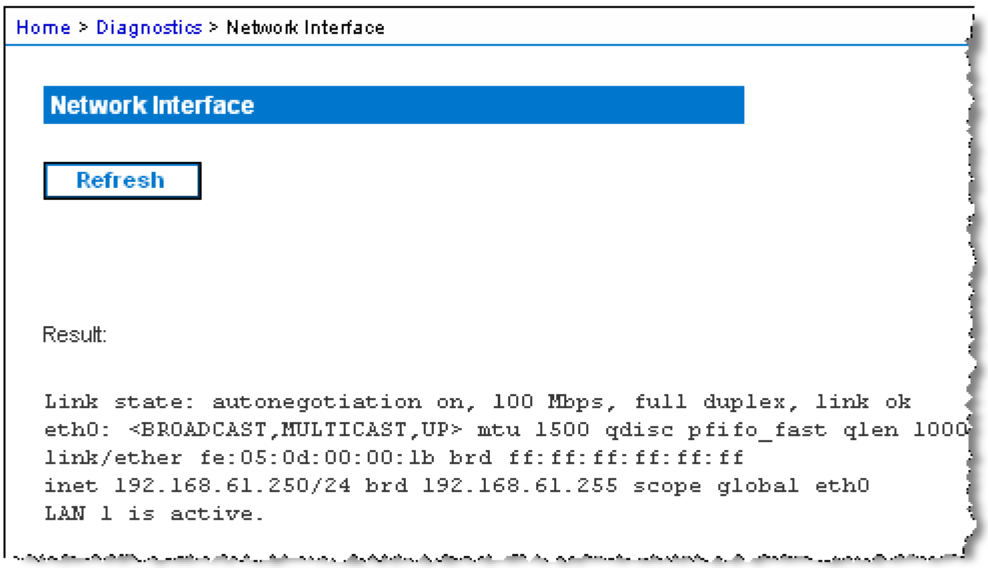
使用：	目的：
Network Interface（网络接口）	获取网络接口的状态。
Network Statistics（网络统计信息）	获取有关网络的统计信息。
Ping Host（Ping 主机）	确定是否可以通过 IP 网络访问特定主机。
Trace Route to Host（跟踪到主机的路由）	确定到所选主机所经过的整个路由。
Device Diagnostics（设备诊断）	在 Raritan 技术支持部门的指示下使用（仅限于远程控制台）。

网络接口页

KX II-101 提供有关网络接口状态的信息。

➢ *查看有关网络接口的信息：*

- 选择 Diagnostics（诊断）> Network Interface（网络接口）。打开 Network Interface（网络接口）页：



显示下列信息：

- Ethernet 接口是工作还是关闭。
- 能否 ping 网关。
- 当前活动的 LAN 端口。

➢ *刷新此信息：*

- 单击 Refresh（刷新）按钮。

网络统计信息页

KX II-101 提供有关网络接口的统计信息。

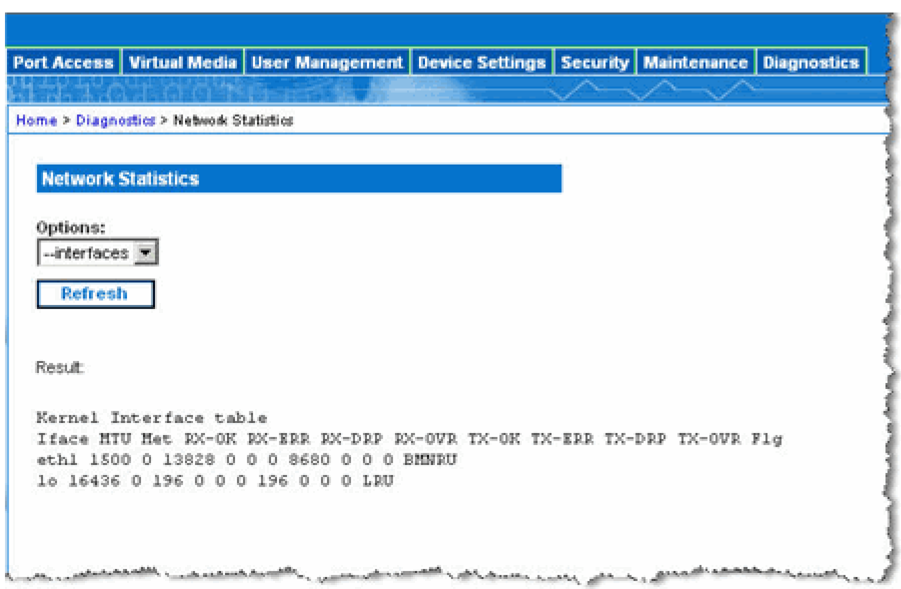
➢ *查看有关网络接口的统计信息：*

1. 选择 Diagnostics（诊断）> Network Statistics（网络统计信息）。打开 Network Statistics（网络统计信息）页。
2. 在 Options（选项）下拉列表上选择适当的选项：

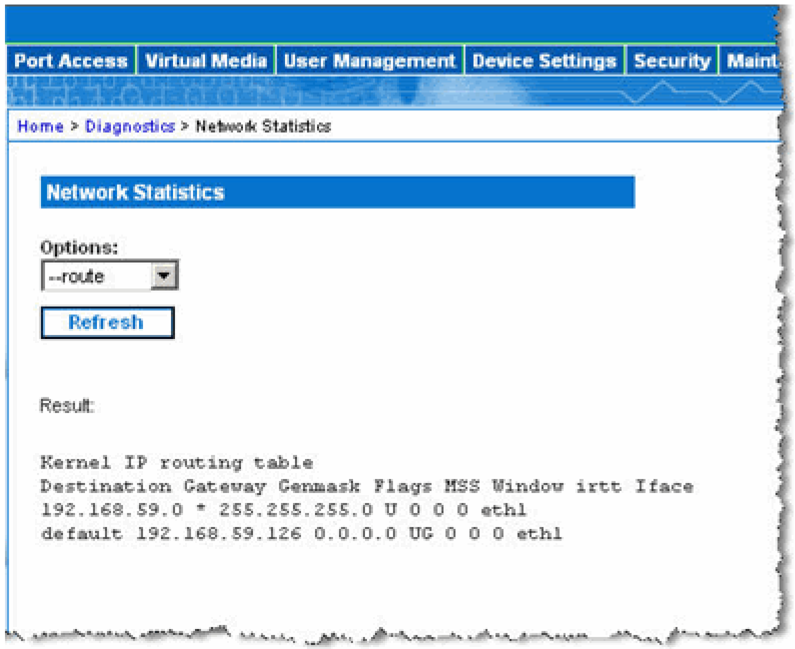
- Statistics（统计信息）。生成类似下面这样的页面：



- Interfaces（接口）。生成类似下面这样的页面：



- Route（路由）。生成类似下面这样的页面：



3. 单击 Refresh（刷新）按钮。

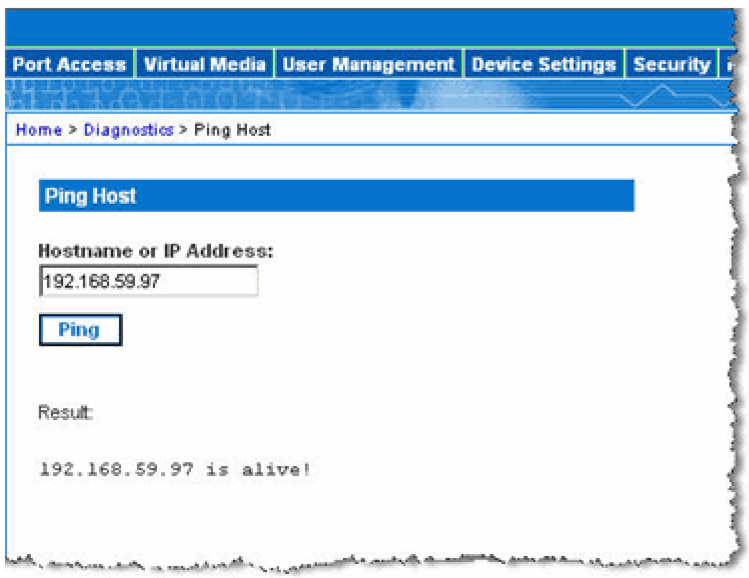
   Result（结果）字段显示相关信息。

Ping 主机页

Ping 是一种网络工具，用于测试是否可以通过 IP 网络访问特定主机或 IP 地址。可以用 Ping Host（Ping 主机）页确定是否可以访问目标服务器或另一台 KX II-101 设备。

➢ *ping 主机：*

1. 选择 Diagnostics（诊断）> Ping Host（Ping 主机）。打开 Ping Host（Ping 主机）页。



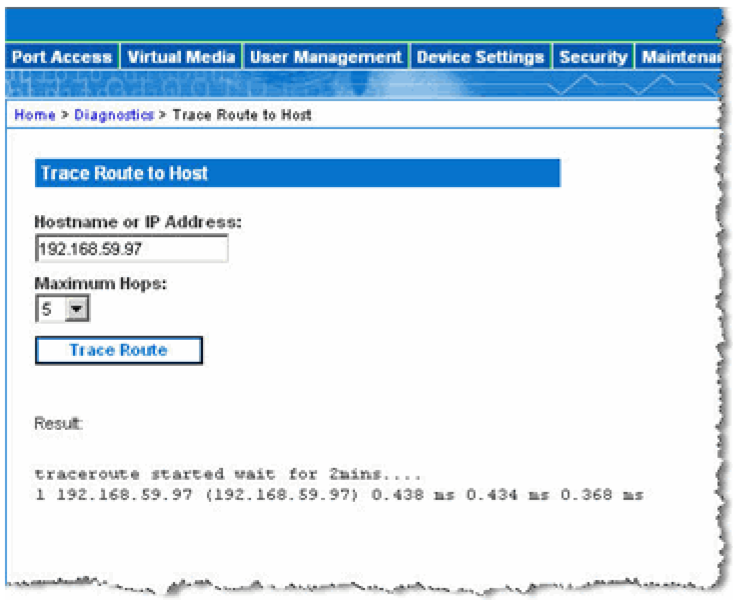
2. 在 Hostname（主机名）字段里输入主机名，或者在 IP Address（IP 地址）字段里输入 IP 地址。
3. 单击 Ping。Result（结果）字段显示 ping 的结果。

跟踪到主机的路由页

跟踪路由是一种网络工具，用于确定到达给定主机名或 IP 地址所经过的整个路由。

➢ *跟踪到主机的路由：*

1. 选择 Diagnostics（诊断）> Trace Route to Host（跟踪到主机的路由）。打开 Trace Route to Host（跟踪到主机的路由）页。



2. 在 Hostname（主机名）字段里输入主机名，或者在 IP Address（IP 地址）字段里输入 IP 地址。
3. 在 Maximum Hops（最大跳数）下拉列表上选择最大跳数（5 到 5，每次递增 5）。
4. 单击 Trace Route（跟踪路由）按钮。针对给定的主机名或 IP 地址与最大跳数执行跟踪路由命令。Result（结果）字段显示跟踪路由的输出。

设备诊断

注意：本页供 Raritan 现场工程师使用，或者在 Raritan 技术支持部门的指导下使用。

Device Diagnostics（设备诊断）页将 KX II-101 上的诊断信息下载到客户机上。无论是否运行 Raritan 技术支持部门提供的可选诊断脚本，均可生成设备诊断日志。诊断脚本生成更多信息，这些信息可用于诊断问题。

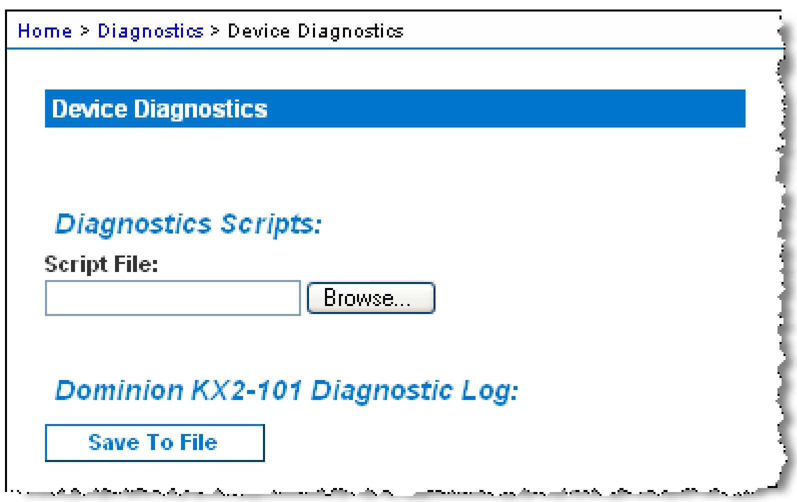
使用下列设置：

- Diagnostics Scripts (optional)（诊断脚本[可选]）。在严重错误调试会话过程中，加载 Raritan 技术支持部门提供的特殊脚本。此脚本被上载到设备上，并在设备上执行。
- Device Diagnostic Log（设备诊断日志）。将 KX II-101 设备上的诊断消息快照下载到客户机上。此加密文件随后被发送到 Raritan 技术支持部门，只有 Raritan 能解密此文件。

注意：只有具备管理权限的用户才能访问本页。

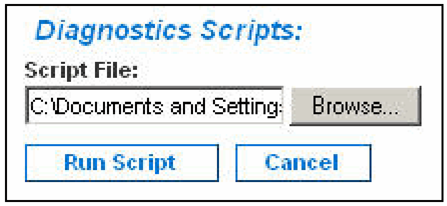
➢ *运行 KX II-101 系统诊断：*

1. 选择 Diagnostics（诊断）> Device Diagnostics（设备诊断）。打开 Device Diagnostics（设备诊断）页。



2. （可选）如果您收到了 Raritan 技术支持部门提供的诊断脚本文件，执行下列步骤。否则，跳到步骤 3。
   a. 必要时检索并解压 Raritan 提供的诊断文件。
   b. 单击 Browse（浏览）按钮。打开 Choose file（选择文件）对话框。
   c. 找到并选择此诊断文件。

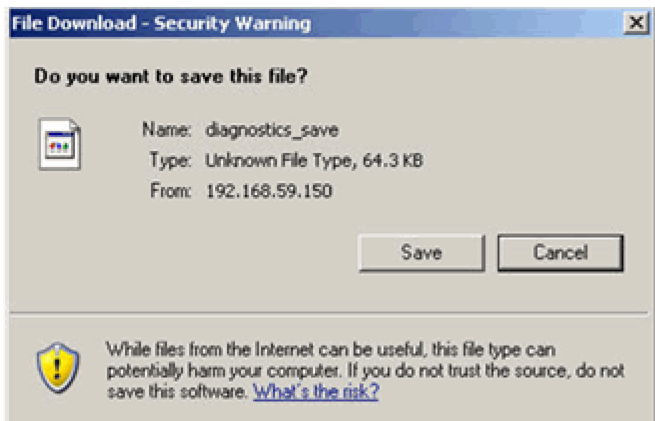
d. 单击 Open（打开）。Script File（脚本文件）字段显示此文件：



e. 单击 Run Script（运行脚本）。

3. 创建诊断文件，把它发送给 Raritan 技术支持部门：

a. 单击 Save to File（保存到文件）按钮。打开 File Download（文件下载）对话框：



b. 单击 Save（保存）。打开 Save As（另存为）对话框。

c. 找到希望的目标，单击 Save（保存）。

4. 根据 Raritan 技术支持部门的指示，用电子邮件发送此文件。

14 取消 CC 管理

在本章内

概述

如果 KX II-101 设备受 CommandCenter Secure Gateway 控制，而您尝试用 KX II-101 Remote Console 直接访问该设备，（在您输入有效用户名和密码之后）显示下列消息：



使 KX II-101 不受 CC-SG 管理

除非 KX II-101 不受 CC-SG 控制，否则不能直接访问该设备。但如果 KX II-101 接收不到来自 CommandCenter 的心跳信号消息（例如 CommandCenter 不联网），您可以解除 CC-SG 对 KX II-101 的控制，以便访问该设备。可以用 CC Unmanage（取消 CC 管理）功能完成这一点。

注意：使用此功能需要维护权限。

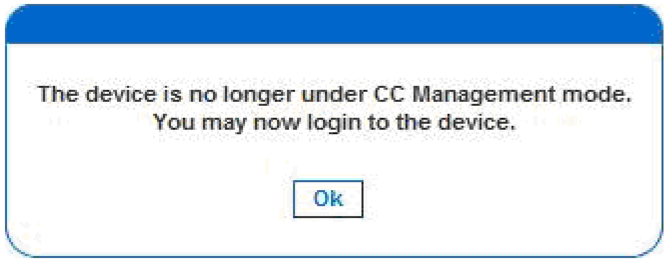
如果接收不到心跳信号消息，在尝试直接访问设备时，显示下列消息：



➢ *使设备不受 CC-SG 管理（使用取消 CC 管理）：*

1. 单击 Yes（是）按钮。系统提示您确认操作：

2. 单击 Yes（是）按钮。显示一条消息，确认该设备不再受 CC 管理：



3. 单击 Yes（是）。打开 KX II-101 登录页。

在代理模式下使用 CC-SG

在 CC-SG 代理模式下不能检测 Virtual KVM Client 版本

在处于代理模式下的 CommandCenter Secure Gateway (CC-SG) 上启动 Virtual KVM Client 时，不知道 Virtual KVM Client 版本。在 About Raritan Virtual KVM Client（关于 Raritan Virtual KVM Client）对话框上，版本显示为 Version Unknown（未知版本）。

代理模式和 MPC

在 CC-SG 配置下使用 KX II-101 时，如果要使用 Multi-Platform Client (MPC)，不要使用 CC-SG 代理模式。

A 规格

在本章内

KX II-101

形状因素	0U 形、水平或垂直机架安装（含支架）
尺寸 **(DxWxH)**	4.055"x 2.913"x 1.063"; 103 x 74 x 27mm
重量	0.6292lbs; 0.286kg
电源	AC/DC (100-240V~/ 6VDC) 电源适配器 或 Power over Ethernet (PoE) Mid-Span Power Insertion Signal-Pair Power Insertion
工作温度	0°-40°C (32°-104°F)
湿度	20%-85% RH
指示灯： 蓝色 RARITAN 背光标志 网络端口	引导状态和功率电平指示灯 网络活动和连接速度指示灯
本地连接	1- Mini USB 端口，用于将 USB 键盘/鼠标和虚拟介质连接到目标服务器 1- MiniDIN9 端口，用于全 RS-232 功能多功能串行端口、调制解调器连接和 Dominion PX 连接
远程连接： 网络协议	1 个 10/100 Ethernet (RJ45) 端口 TCP/IP、HTTP、HTTPS、UDP、RADIUS、LDAP、SNTP 和 DHCP

屏幕分辨率： PC 图形模式 SUN® 视频模式	720x400 (DOS) 640 X 480 @ 60/72/75/85Hz, 800 X 600 @ 56/60/72/75/85Hz, 1024 X 768 @ 60/70/75/85Hz, 1152 X 864 @ 60/75Hz, 1280 X 1024 @ 60Hz, 1600 X 1200 @ 60Hz
认证：	UL/CUL、FCC Class A、CB、CE Class A 和 VCCI Class A

连接器

接口类型	长度（英寸；cm）	说明
视频	15"; 38 cm	集成电缆
PS/2	15"; 38 cm	集成电缆
Mini-USB 到 USB(M)	17.7"; 45 cm	USB 电缆
MiniDin9(M) 到 DB9(F)	72"; 182 cm	串行电缆
DKX2-101-LPKVMC	3.9"; 10 cm	本地端口集成电缆
DKX2-101-SPDUC	70.86"; 180 cm	用于连接 Dominion PX 的电缆

Raritan Remote Client 软件

操作系统要求：Windows XP/NT/ME/2000

B 机架安装

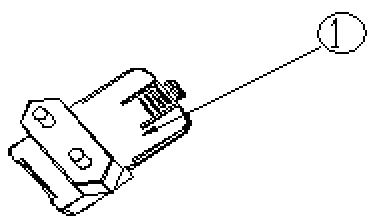
KX II-101 设备可以垂直或水平安装在服务器机架的任一边，既可以面对面安装，也可以面向同一个方向安装。使用随 KX II-101 一起提供的支架和螺丝。

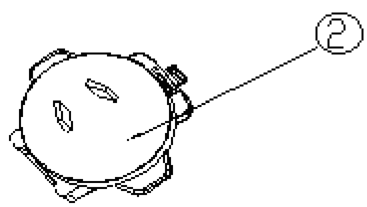
在本章内

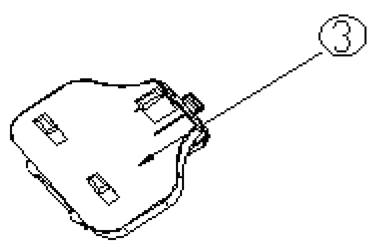
AC-DC 适配器固定夹

标志夹类型

1. 欧盟夹
2. 澳大利亚夹
3. 英国夹

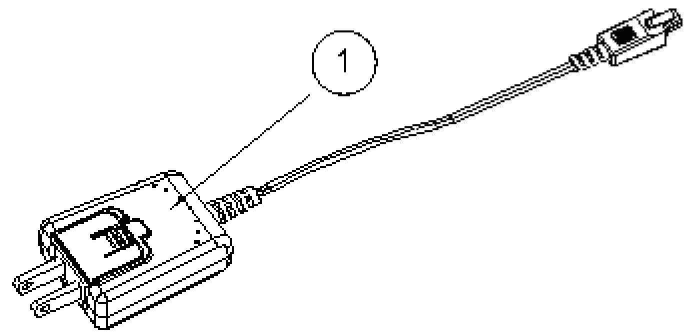


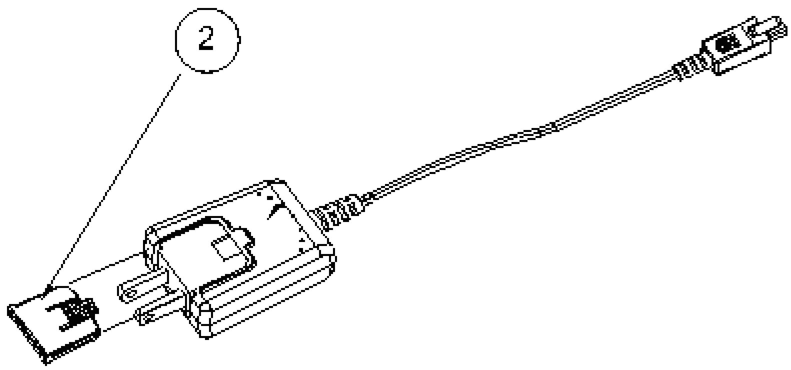




取下 AC-DC 电源适配器盖子

1. AC/DC 电源适配器
2. 盖子。推动卸下。

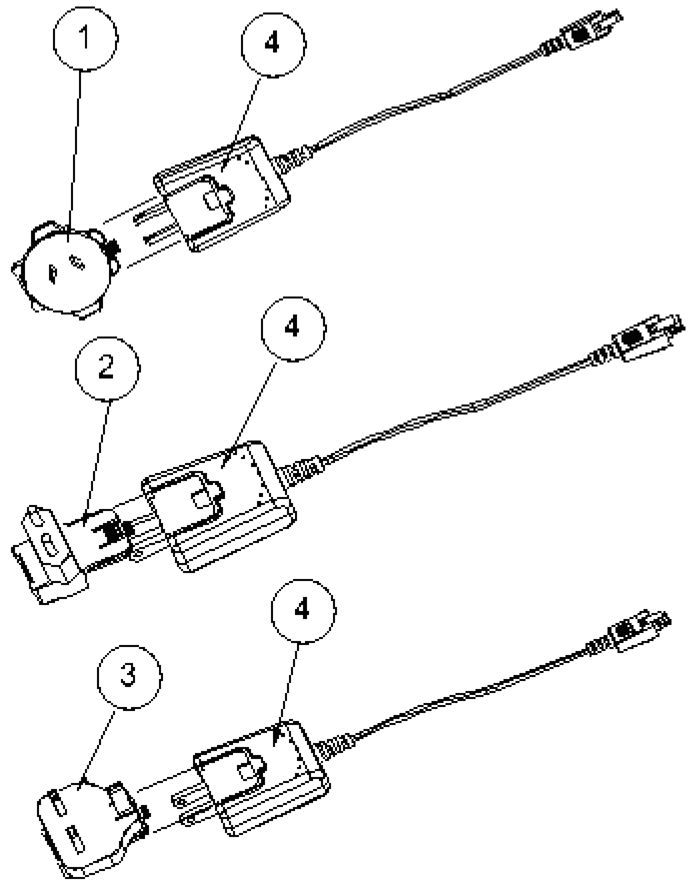




连接 AC-DC 电源适配器夹

1. 澳大利亚夹
2. 欧盟夹
3. 英国夹

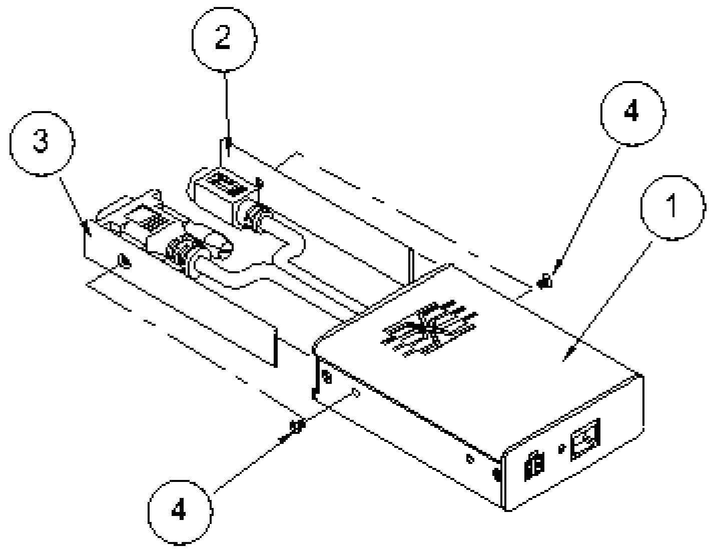
4. 电源适配器



支架安装

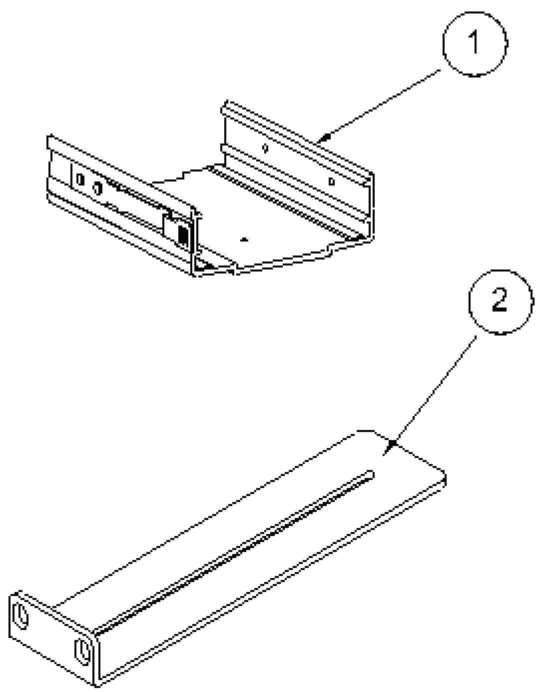
1. KX II-101 设备
2. 右面板
3. 左面板
4. 螺丝

- 取下 KX II-101 设备上的螺丝。
- 将 KX II-101 设备的左右面板滑出来。



KX II-101 支架零件

1. U 型支架
2. L 型支架

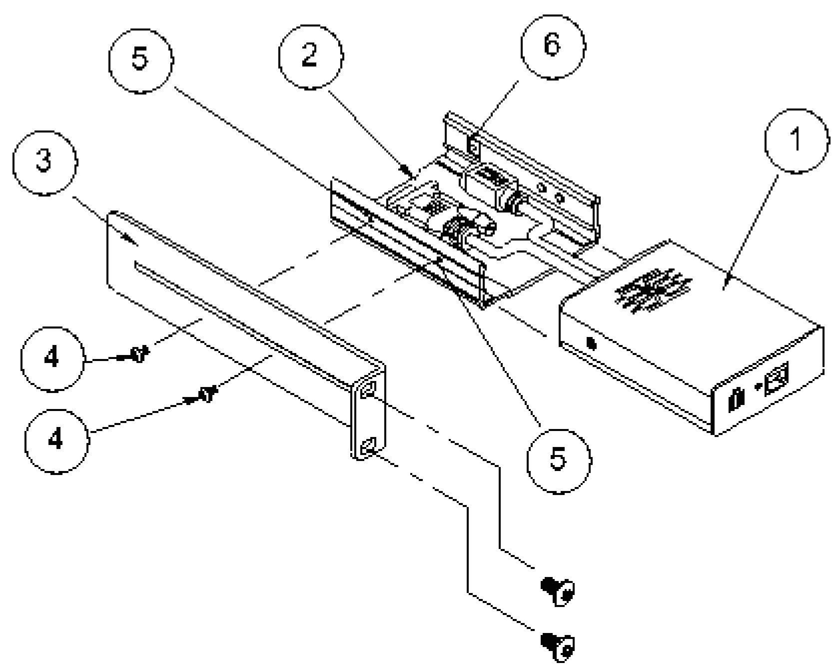


将水平安装支架固定在 KX II-101 上

1. KX II-101 设备
2. U 型支架
3. L 型支架
4. 螺丝
5. 安装孔
6. 闩杆

- 用随附的螺丝将 U 型支架固定在 L 型支架上。调整支架位置，拧紧螺丝。
- 用（机架制造商提供的）机架安装螺丝将 U 型支架和 L 型支架总成安装在机架上。
- 将 KX II-101 滑进 U 型支架，KVM 导线面向目标服务器。拉出并释放闩杆，将 KX II-101 设备锁进 U 型支架。

下图说明将 KX II-101 安装在左边。如要将 KX II-101 安装在右边，可遵循上述说明，但将支架安装在 KX II-101 设备的右边。



将垂直安装支架固定在 KX II-101 上

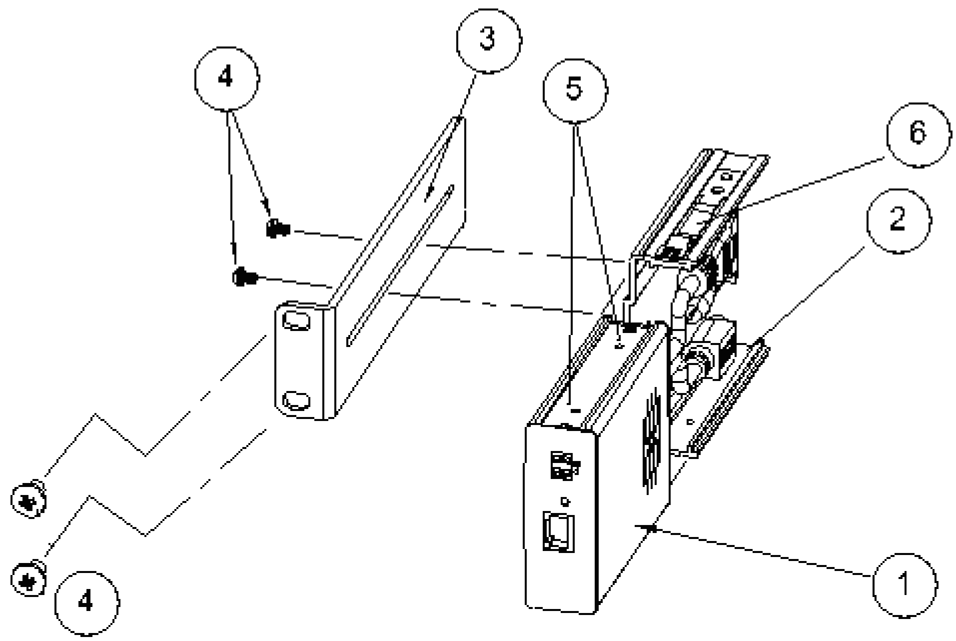
1. KX II-101 设备
2. U 型支架

3. L 型支架
4. 螺丝
5. 安装孔
6. 闩杆

用随附的螺丝将 U 型支架固定在 L 型支架上。调整支架位置，拧紧螺丝。

用（机架制造商提供的）机架安装螺丝将 U 型支架和 L 型支架总成安装在机架上。

将 KX II-101 滑进 U 型支架，KVM 导线面向目标服务器。拉出并释放闩杆，将 KX II-101 设备锁进 U 型支架。



索引

ZH

W

R

J

F

D

B

SH

Y

D

M

CH

R

G

CH

T

Z

A

SH

Y

J

W

M

➢ *美国/加拿大/拉丁美洲*

周一至周五
8 a.m. - 8 p.m.（东部时间）
电话：800-724-8090 或 732-764-8886
有关 CommandCenter NOC：按 6，然后按 1
有关 CommandCenter Secure Gateway：按 6，然后按 2
传真:732-764-8887
有关 CommandCenter NOC 的电子邮件：tech-ccnoc@raritan.com
有关所有其他产品的电子邮件：tech@raritan.com

➢ *中国*

北京

周一至周五
9 a.m. - 6 p.m.（当地时间）
电话：+86-10-88091890

上海

周一至周五
9 a.m. - 6 p.m.（当地时间）
电话：+86-21-5425-2499

广州

周一至周五
9 a.m. - 6 p.m.（当地时间）
电话：+86-20-8755-5561

➢ *印度*

周一至周五
9 a.m. - 6 p.m.（当地时间）
电话：+91-124-410-7881

➢ *日本*

周一至周五
9:30 a.m. - 5:30 p.m.（当地时间）
电话：+81-3-3523-5994
电子邮件：support.japan@raritan.com

➢ *欧洲*

欧洲

周一至周五
8:30 a.m. - 5 p.m. GMT+1（中部欧洲时间）
电话：+31-10-2844040
电子邮件：tech.europe@raritan.com

英国

周一至周五
8:30 a.m. - 5 p.m. GMT+1（中部欧洲时间）
电话：+44-20-7614-77-00

法国

周一至周五
8:30 a.m. - 5 p.m. GMT+1（中部欧洲时间）
电话：+33-1-47-56-20-39

德国

周一至周五
8:30 a.m. - 5 p.m. GMT+1（中部欧洲时间）
电话：+49-20-17-47-98-0

➢ *韩国*

周一至周五
9 a.m. - 6 p.m.（当地时间）
电话：+82-2-5578730

➢ *澳大利亚墨尔本*

周一至周五
9:00 a.m. - 6 p.m.（当地时间）
电话：+61-3-9866-6887

➢ *台湾*

周一至周五
9 a.m. - 6 p.m. GMT-5（标准）GMT-4（夏令时）
电话：+886-2-8919-1333
电子邮件：tech.rap@raritan.com